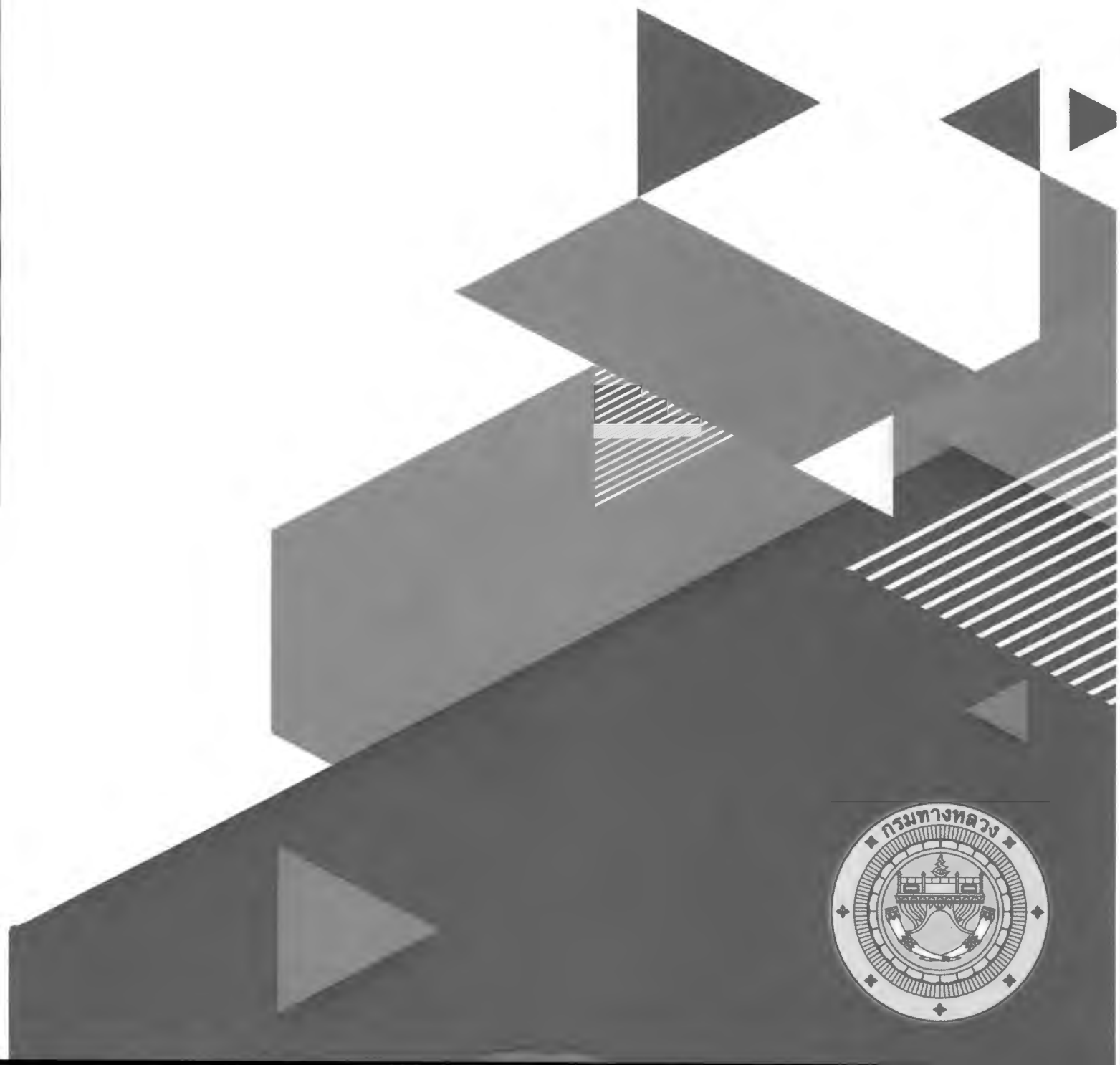
แผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหา ด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมทางหลวง พ.ศ.๒๕๖๒



สารบัญ

บทที่ ๑
บทนำ

๑.๑ เจตนารมณ์ของยุทธศาสตร์ชาติ

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทยมาตรา ๖๕ กำหนดให้รัฐจัดให้มียุทธศาสตร์ชาติเป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืนตามหลักธรรมาภิบาลให้สอดคล้องและบูรณาการกันเพื่อให้เกิดพลังผลักดันร่วมกันไปสู่เป้าหมาย โดยยุทธศาสตร์ชาติ ๒๐ ปี พ. ศ. ๒๕๖๑ – ๒๕๖๔ เป็นยุทธศาสตร์ชาติฉบับแรกของประเทศไทยตามรัฐธรรมนูญซึ่งจะต้องนำไปสู่การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนา ตามปรัชญาของเศรษฐกิจพอเพียง” นำไปสู่การพัฒนาให้คนไทยมีความสุข และตอบสนองตอบต่อการบรรลุ ซึ่งผลประโยชน์แห่งชาติ ในการที่จะพัฒนาคุณภาพชีวิต สร้างรายได้ระดับสูง เป็นประเทศพัฒนาแล้ว และสร้างความสุขของ คนไทย สังคมมีความมั่นคงเสมอภาคและ เป็นธรรม ประเทศสามารถแข่งขันได้ในระบบ เศรษฐกิจ ประกอบด้วย ๖ ยุทธศาสตร์ ได้แก่

(๑) ยุทธศาสตร์ชาติด้านความมั่นคง

(๒) ยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน

(๓) ยุทธศาสตร์ชาติด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์

(๔) ยุทธศาสตร์ชาติด้านการสร้างโอกาสและความเสมอภาคทางสังคม

(๕) ยุทธศาสตร์ชาติด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม และ

(๖) ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

๑.๒ เจตนารมณ์ของยุทธศาสตร์ชาติด้านความมั่นคง

ยุทธศาสตร์ด้านความมั่นคง มีเป้าหมายการพัฒนาที่สำคัญ คือ ประเทศชาติมั่นคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคง ปลอดภัย เอกราชอธิปไตย และมีความสงบเรียบร้อยในทุกระดับ ตั้งแต่ระดับชาติ สังคม ชุมชน มุ่งเน้นการพัฒนาคนเครื่องมือ เทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่ให้มีความพร้อมสามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบ และทุกระดับความรุนแรง ควบคู่ไปกับการป้องกันและแก้ไขปัญหาด้านความมั่นคงที่มีอยู่ในปัจจุบัน และที่อาจจะเกิดขึ้นในอนาคต ใช้กลไกการแก้ไขปัญหาแบบบูรณาการทั้งกับส่วนราชการ ภาคเอกชน ประชาสังคม และองค์กรที่ไม่ใช่รัฐ รวมถึงประเทศเพื่อนบ้านและมิตรประเทศทั่วโลกบนพื้นฐานของหลักธรรมาภิบาล เพื่อเอื้ออำนวยประโยชน์ต่อการดำเนินการของยุทธศาสตร์ชาติด้านอื่น ๆ ให้สามารถขับเคลื่อนไปได้ตามทิศทางและเป้าหมายที่กำหนด โดยมีประเด็นยุทธศาสตร์ ๕ ประเด็น ได้แก่

(๑) การรักษาความสงบภายในประเทศ กำหนดประเด็นย่อย ดังนี้ พัฒนาและเสริมสร้างคนในทุกภาคส่วนให้มีความเข้มแข็ง มีความพร้อม พัฒนาและเสริมสร้างความจงรักภักดีต่อสถาบันหลักของชาติ พัฒนาและเสริมสร้างการเมืองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขที่มีเสถียรภาพและมีธรรมาภิบาล เห็นแก่ประโยชน์ของประเทศชาติมากกว่าประโยชน์ส่วนตน ตระหนักในเรื่องความมั่นคง

และมีส่วนร่วมในการแก้ไขปัญหา และการพัฒนาและเสริมสร้างกลไกที่สามารถป้องกันและขจัดสาเหตุของประเด็นปัญหาความมั่นคงที่สำคัญ

(๒) การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง กำหนดประเด็นย่อย ดังนี้ การแก้ไขปัญหาความมั่นคงในปัจจุบัน การติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่ การสร้างความปลอดภัยและความสันติสุขอย่างถาวรในพื้นที่จังหวัดชายแดนภาคใต้ การรักษาความมั่นคงและผลประโยชน์ทางทรัพยากรธรรมชาติและสิ่งแวดล้อมทั้งทางบกและทางทะเล

(๓) การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติ กำหนดประเด็นย่อย ดังนี้ การพัฒนาระบบงานข่าวกรองแห่งชาติแบบบูรณาการอย่างมีประสิทธิภาพ การพัฒนาและผนึกพลังอำนาจแห่งชาติ กองทัพและหน่วยงานความมั่นคงรวมทั้งภาครัฐและภาคประชาชน ให้พร้อมป้องกันและรักษาอธิปไตยของประเทศ และเผชิญกับภัยคุกคามได้ทุกมิติทุกรูปแบบและทุกระดับ และการพัฒนาระบบเตรียมพร้อมแห่งชาติและการบริหารจัดการภัยคุกคามให้มีประสิทธิภาพ

(๔) การบูรณาการความร่วมมือด้านความมั่นคงกับอาเซียนและนานาชาติ รวมถึงองค์กรภาครัฐและที่มิใช่ภาครัฐ กำหนดประเด็นย่อย ดังนี้ การเสริมสร้างและรักษาดุลยภาพสภาวะแวดล้อมระหว่างประเทศ การเสริมสร้างและธำรงไว้ซึ่งสันติภาพและความมั่นคงของภูมิภาค การร่วมมือทางการพัฒนากับประเทศเพื่อนบ้าน ภูมิภาค โลก รวมถึงองค์กรภาครัฐและที่มิใช่ภาครัฐ

(๕) การพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม กำหนดประเด็นย่อย ดังนี้ การพัฒนากลไกให้พร้อมสำหรับการติดตาม เฝ้าระวัง แจ้งเตือน ป้องกันและแก้ไขปัญหาความมั่นคงแบบองค์รวมอย่างเป็นรูปธรรม การบริหารจัดการความมั่นคงให้เอื้ออำนวยต่อการพัฒนาประเทศในมิติอื่น ๆ และการพัฒนากลไกและองค์กรขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคง

๑.๓ เจตนารมณ์ของแผนแม่บทเพื่อบรรลุเป้าหมายตามยุทธศาสตร์ชาติ

มีกลไกบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ระดับชาติ แก้ไขปัญหาแบบองค์รวมทั้งการรับมือกับเหตุการณ์ทั่วไป อาชญากรรมทางไซเบอร์ และรับมือกับภัยคุกคามทางไซเบอร์ที่มีผลกระทบต่อเศรษฐกิจและสังคม และความมั่นคงของประเทศ ทั้งในระยะสั้นและระยะยาวอย่างเป็นรูปธรรมและยั่งยืน โดยกำหนดองค์กรรับผิดชอบระดับชาติดำเนินการ มีแผนการขับเคลื่อนที่เป็นรูปธรรม และกำหนดการบริหารจัดการแบบองค์รวมในระดับชาติให้สอดคล้องไปในทิศทางเดียวกัน และสอดรับกับเจตนารมณ์ของยุทธศาสตร์ชาติ

๑.๔ นโยบาย และแผนอื่น ๆ ที่เกี่ยวข้องและส่งเสริมต่อยุทธศาสตร์ชาติด้านความมั่นคง

๑.๔.๑ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐-๒๕๖๔)

<u>วัตถุประสงค์</u>

- เพื่อวางรากฐานให้คนไทยเป็นคนที่สมบูรณ์ มีคุณธรรมจริยธรรม มีระเบียบวินัย ค่านิยมที่ดี มีจิตสาธารณะ และมีความสุข โดยมีสุขภาวะและสุขภาพที่ดี ครอบครัวอบอุ่น ตลอดจนเป็นคนเก่งที่มีทักษะความรู้ความสามารถและพัฒนาตนเองได้ต่อเนื่องตลอดชีวิต

- เพื่อให้คนไทยมีความมั่นคงทางเศรษฐกิจและสังคม ได้รับความเป็นธรรมในการเข้าถึงทรัพยากรและบริการทางสังคมที่มีคุณภาพ ผู้ด้อยโอกาสได้รับการพัฒนาศักยภาพ รวมทั้งชุมชนมีความเข้มแข็งพึ่งพาตนเองได้

- เพื่อให้เศรษฐกิจเข้มแข็ง แข่งขันได้ มีเสถียรภาพ และมีความยั่งยืน สร้างความเข้มแข็งของฐานการผลิตและบริการเดิมและขยายฐานใหม่ โดยการใช้นวัตกรรมที่เข้มข้นมากขึ้น สร้างความเข้มแข็งของ เศรษฐกิจฐานราก และสร้างความมั่นคงทางพลังงาน อาหาร และน้ำ

- เพื่อรักษาและฟื้นฟูทรัพยากรธรรมชาติและคุณภาพสิ่งแวดล้อม ให้สามารถสนับสนุนการเติบโตที่เป็นมิตรกับสิ่งแวดล้อมและการมีคุณภาพชีวิตที่ดีของประชาชน

- เพื่อให้การบริหารราชการแผ่นดินมีประสิทธิภาพ โปร่งใส ทันสมัย และมีการทำงานเชิงบูรณาการของภาคีการพัฒนา

- เพื่อให้มีการกระจายความเจริญไปสู่ภูมิภาคโดยการพัฒนาภาคและเมือง เพื่อรองรับการพัฒนายกระดับฐานการผลิตและบริการเดิมและขยายฐานการผลิตและบริการใหม่

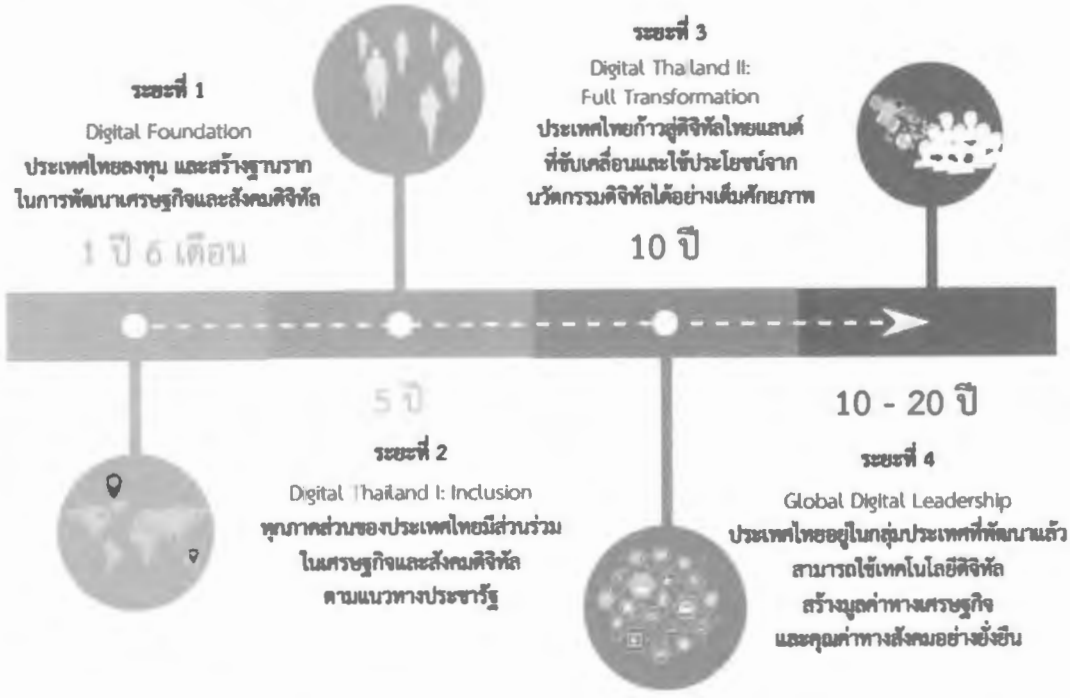
- เพื่อผลักดันให้ประเทศไทยมีความเชื่อมโยง (Connectivity) กับประเทศต่างๆ ทั้งในระดับอนุภูมิภาค ภูมิภาคและนานาชาติได้อย่างสมบูรณ์และมีประสิทธิภาพ รวมทั้งให้ประเทศไทยมีบทบาทนาและสร้างสรรค์ด้านการค้า การบริการและการลงทุน ภายใต้กรอบความร่วมมือต่างๆ ทั้งในระดับอนุภูมิภาค ภูมิภาค และโลก

<u>ยุทธศาสตร์</u>

- ยุทธศาสตร์ที่ ๑ การเสริมสร้างและพัฒนาศักยภาพทุนมนุษย์
- ยุทธศาสตร์ที่ ๒ การสร้างความเป็นธรรมและลดความเหลื่อมล้ำในสังคม
- ยุทธศาสตร์ที่ ๓ การสร้างความเข้มแข็งทางเศรษฐกิจและแข่งขันได้อย่างยั่งยืน
- ยุทธศาสตร์ที่ ๔ การเติบโตที่เป็นมิตรกับสิ่งแวดล้อมเพื่อการพัฒนาอย่างยั่งยืน
- ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน
- ยุทธศาสตร์ที่ ๖ การบริหารจัดการในภาครัฐ การป้องกันการทุจริตประพฤติมิชอบและธรรมาภิบาลในสังคมไทย
- ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์
- ยุทธศาสตร์ที่ ๘ การพัฒนาวิทยาศาสตร์ เทคโนโลยี วิจัย และนวัตกรรม
- ยุทธศาสตร์ที่ ๙ การพัฒนาภาค เมือง และพื้นที่เศรษฐกิจ
- ยุทธศาสตร์ที่ ๑๐ ความร่วมมือระหว่างประเทศเพื่อการพัฒนา

๑.๔.๒ แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ๒๐ ปี (๒๕๕๙-๒๕๗๙)

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมได้รับความเห็นชอบจากคณะรัฐมนตรีเมื่อวันที่ ๕ เมษายน ๒๕๕๙ ได้กำหนดทิศทางการพัฒนาประเทศในยุคเศรษฐกิจและสังคมดิจิทัลไว้ ๖ ยุทธศาสตร์ คือ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล การสร้างสังคมคุณภาพที่ทั่วถึงและเท่าเทียมด้วยเทคโนโลยีดิจิทัล การปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล การพัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล และการสร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล ซึ่งเป้าหมายในระยะ ๑๐ ปีของแผนฯ ฉบับนี้ได้ระบุไว้ชัดเจนว่าจะต้องปฏิรูปกระบวนทัศน์การทำงานและการให้บริการของภาครัฐด้วยเทคโนโลยีดิจิทัล เพื่อนำประเทศไทยไปสู่กลุ่ม ๕๐ ประเทศแรกที่มีการพัฒนาด้านรัฐบาลดิจิทัลสูงสุด โดยได้แบ่งระยะการพัฒนาไว้ ๔ ระยะดังแสดงในภาพ



ระยะที่ ๑ Digital Foundataion : แผนฯ ในระยะแรกนี้กำหนดให้หน่วยงานภาครัฐมีการทำงานที่เชื่อมโยงและบูรณาการข้อมูลข้ามหน่วยงาน มีชุดข้อมูลและระบบบริการพื้นฐานภาครัฐ (government service platform) ที่มีมาตรฐาน สามารถเข้าถึง แลกเปลี่ยน เชื่อมโยง และใช้งานร่วมกันได้

ระยะที่ ๒ Digital Thailand I (Inclusion) : การทำงานระหว่างภาครัฐจะเชื่อมโยงและบูรณาการเหมือนเป็นองค์กรเดียว กล่าวคือมีการบูรณาการข้อมูลข้ามหน่วยงานโดยสมบูรณ์ ผู้บริหารภาครัฐสามารถเข้าถึงข้อมูลได้ทุกระดับ และใช้ประโยชน์จากการวิเคราะห์ข้อมูลขนาดใหญ่เพื่อประกอบการวางแผนและการตัดสินใจอย่างถูกต้อง ทันสถานการณ์ และตรงตามความต้องการของประชาชนหรือผู้ใช้บริการ (citizen driven) โดยประชาชนจะมีส่วนร่วมในการตัดสินใจเชิงนโยบายผ่านทางอิเล็กทรอนิกส์ (connected governance) ได้อย่างสะดวก และสามารถเข้าถึงข้อมูลที่มีความน่าเชื่อถือ มั่นคงปลอดภัย มีความเป็นส่วนตัว และสามารถตรวจสอบได้ และนำไปสู่การดำเนินงานที่มีความโปร่งใส

ระยะที่ ๓ Digital Thailand II (Full Transformation): ในระยะนี้ประเทศไทยจะก้าวสู่ดิจิทัลไทยแลนด์ โดยการจัดให้มีบริการภาครัฐที่ขับเคลื่อนโดยความต้องการของประชาชน โดยการเชื่อมโยงประชาชนให้เข้าถึงข้อมูลและมีส่วนร่วมในการกำหนดแนวทางการบริหารจัดการภาครัฐ ตลอดจนการพัฒนาสังคมและเศรษฐกิจ โดยรัฐจะต้องมีบริการสาธารณะในลักษณะอัตโนมัติ (automated public services) ตามหลักการออกแบบที่เป็นสากล (universal design) ผ่านระบบดิจิทัลที่สอดคล้องกับสถานการณ์และความต้องการของผู้รับบริการแต่ละบุคคล โดยผู้ใช้งานไม่ต้องร้องขอต่อรัฐ การกำหนดนโยบายและการตัดสินใจตั้งอยู่บนพื้นฐานข้อมูลที่ทันสมัย มีการวิเคราะห์ข้อมูลขนาดใหญ่ และการมีส่วนร่วมของประชาชน

ระยะที่ ๔ Global Digital Leadership: ในระยะ ๑๐ ปีสุดท้ายของภูมิทัศน์ดิจิทัล ประเทศไทยจะก้าวเข้าสู่การเป็นประเทศที่พัฒนาแล้ว บทบาทของภาครัฐจะปรับเปลี่ยนไปเป็นผู้อำนวยความสะดวกในการสร้างบริการสาธารณะโดยเอกชนและประชาชน โดยประชาชนทุกคนสามารถเข้าถึงบริการได้โดยไม่มีข้อจำกัดทางกายภาพ พื้นที่ และภาษา ทำให้ประเทศไทยเป็นผู้นำด้านรัฐบาลดิจิทัลทั้งการบริหารจัดการรัฐและบริการประชาชนในภูมิภาคอาเซียน

นอกจากทิศทางของการพัฒนาภาครัฐแล้ว แผนพัฒนาดิจิทัลฯ นี้ยังได้ให้ความสำคัญของการพัฒนากำลังคนอีกด้วย เนื่องจากการขับเคลื่อนแผนฯ ในทิศทางต่าง ๆ จะไม่สามารถสำเร็จได้เลยหากไม่มีการพัฒนาสมรรถนะด้านเทคโนโลยีสารสนเทศของทรัพยากรมนุษย์ภายในประเทศ ดังนั้น ในฐานะผู้บริหารเทคโนโลยีสารสนเทศของรัฐ จะต้องมีความเข้าใจและสามารถวางแผนยุทธศาสตร์การนำเทคโนโลยีดิจิทัลไปพัฒนาภารกิจขององค์กร โดยต้องสอดคล้องกับสถาปัตยกรรมองค์กรของหน่วยงาน ตลอดจนสามารถสร้างประโยชน์จากการบูรณาการเชื่อมโยงข้อมูลขององค์กรกับหน่วยงานภาครัฐอื่นได้

แนวทางพัฒนาภาครัฐที่กำหนดโดยแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมฉบับนี้สะท้อนให้เห็นถึงความสำคัญของการบูรณาการข้อมูลภายในและภายนอกหน่วยงาน ซึ่งทิศทางการพัฒนานั้นระบุไว้ชัดเจนว่าจะต้องเน้นการเชื่อมโยงภาครัฐให้เป็นอันหนึ่งอันหนึ่งเดียวทั้งในแง่กระบวนการปฏิบัติงาน ระบบการให้บริการ และข้อมูล นอกจากนี้เป้าหมายสูงสุดของการให้บริการนั้นยังอยู่ที่การมีส่วนร่วมของประชาชนเป็นสำคัญ

๑.๔.๓ แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ของกระทรวงคมนาคม ระยะ ๕ ปี (ปีงบประมาณ ๒๕๖๐-๒๕๖๔)

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ของกระทรวงคมนาคมฯ หรือ แผนพัฒนาคมนาคมดิจิทัล ๒๐๒๑ เป็นกรอบชี้นำการนำเทคโนโลยีดิจิทัลที่มีแนวโน้มจะเข้ามีอิทธิพล (Digital Technology Trends) กับระบบคมนาคมและขนส่งของไทยในอนาคต มาสร้างนวัตกรรมด้านคมนาคมขนส่งใน ๓ ด้าน ประกอบด้วย

๑) นวัตกรรมด้านตำแหน่งเชิงยุทธศาสตร์ (Position Innovation)

๒) นวัตกรรมด้านผลิตภัณฑ์และบริการ (Product & Process Innovation)

๓) นวัตกรรมด้านกรอบความคิด (Paradigm Innovation)

โดยมีจุดมุ่งหมายสำคัญ คือ การมุ่งยกระดับคุณค่าทางเศรษฐกิจและสังคมอย่างก้าวกระโดด (Disruptive Innovation) เพื่อขับเคลื่อน (Enabler) ระบบคมนาคมขนส่งให้บรรลุเป้าประสงค์ ทั้งในด้านการขนส่งที่ปลอดภัย เป็นมิตรต่อสิ่งแวดล้อม (Green and Safe Transport) มีประสิทธิภาพ (Transport Efficiency) สามารถเข้าถึงได้อย่างเสมอภาคและเท่าเทียม (Inclusivity)

๑.๔.๔ แผนยุทธศาสตร์กรมทางหลวง พ.ศ.๒๕๖๐-๒๕๖๔

วิสัยทัศน์

"ระบบทางหลวงที่สะดวกปลอดภัย เชื่อมโยงการพัฒนาโครงสร้างพื้นฐานของประเทศ"

เป้าหมายการให้บริการ

๑) การพัฒนาระบบทางหลวงให้เชื่อมต่อ เข้าถึงและคล่องตัว เพื่อระบบการเดินทางขนส่งและโลจิสติกส์ที่สมดุลและสมบูรณ์

๒) การพัฒนาและบำรุงรักษาระดับการให้บริการของระบบทางหลวงที่รวดเร็วครอบคลุมและทันต่อสถานการณ์

๓) การควบคุมและพัฒนามาตรฐานความปลอดภัยบนระบบทางหลวงอย่างบูรณาการเพื่อยกระดับคุณภาพชีวิตของประชาชนและลดการสูญเสียทางเศรษฐกิจ

๔) การพัฒนาระบบบริการจัดการองค์กรตามหลักธรรมาภิบาลอย่างต่อเนื่องเพื่อเชื่อมโยงความสมดุลทางด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม

ค่านิยม

H : HIGH PERFORMANCE สร้างสรรค์ผลงาน
I : INTELLIGENT TECHNOLOGY ผสานเทคโนโลยี
G : GOOD KNOWLEDGE ด้วยความรู้ที่เหมาะสม
H : HONESTY ซื่อสัตย์
W : WORK SMART ปฏิบัติงานอย่างรู้รอบ
A : ACCOUNTABILITY รับผิดชอบต่อพันธกิจ
Y : YEAR-ROUND COMMITMENT เกาะติดการให้บริการ
S : SYNERGY ทำงานร่วมกันเป็นหนึ่งเดียว

ยุทธศาสตร์

- ยุทธศาสตร์ที่ ๑ การพัฒนาระบบทางหลวงให้เชื่อมต่อ เข้าถึง และคล่องตัวเพื่อระบบการเดินทางขนส่งและโลจิสติกส์สมดุลและสมบูรณ์

- ยุทธศาสตร์ที่ ๒ การพัฒนาและบำรุงรักษาระดับการให้บริการของระบบทางหลวงที่รวดเร็ว ครอบคลุม และทันต่อสถานการณ์

- ยุทธศาสตร์ที่ ๓ การควบคุมและพัฒนามาตรฐานความปลอดภัยบนระบบทางหลวงอย่างบูรณาการ เพื่อยกระดับคุณภาพชีวิตของประชาชนและลดการสูญเสียทางเศรษฐกิจ

- ยุทธศาสตร์ที่ ๔ การพัฒนาระบบบริหารจัดการองค์กรตามหลักธรรมาภิบาลอย่างต่อเนื่องเพื่อเชื่อมโยงความสมดุลทางด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม

๑.๔.๕ แผนปฏิบัติการดิจิทัลกรมทางหลวง ปี พ.ศ.๒๕๖๐-๒๕๖๔

กรมทางหลวง จัดทำแผนปฏิบัติการดิจิทัล กรมทางหลวง ปี พ.ศ.๒๕๖๐-๒๕๖๔ เพื่อใช้เป็นกรอบในการดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ขับเคลื่อนยุทธศาสตร์ของกรมทางหลวง และยุทธศาสตร์การพัฒนาดิจิทัลของประเทศไทย ในระยะเวลา ๕ ปีข้างหน้า โดยดำเนินการให้เกิดความเหมาะสมกับผลการดำเนินการด้านเทคโนโลยีสารสนเทศของกรมทางหลวงที่ผ่านมาและผลกระทบจากการเปลี่ยนแปลงของเทคโนโลยีและปัจจัยอื่นๆ

เป้าหมายโดยรวมของการพัฒนา ICT ของกรมทางหลวง

๑) ระบบเทคโนโลยีสารสนเทศและการสื่อสารช่วยสนับสนุนและส่งเสริมให้กรมทางหลวงสามารถดำเนินการตามภารกิจ ได้อย่างมีประสิทธิภาพ

(๑) โครงสร้างพื้นฐานด้าน ICT ของกรมทางหลวงทั้งหน่วยงานส่วนกลางและภูมิภาคมีความมั่นคง ปลอดภัย และสามารถรองรับการปฏิบัติงานได้เป็นอย่างดี

(๒) ข้อมูลและสารสนเทศของกรมทางหลวง สามารถบูรณาการและเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศและหน่วยงานที่เกี่ยวข้อง

(๓) กรมทางหลวงเป็นหน่วยงานที่สามารถบริหารจัดการและการปฏิบัติงานด้าน ICT อย่างมีประสิทธิภาพ

๒) ระบบสารสนเทศเพื่อการบริหารจัดการของกรมทางหลวง มีคุณภาพสูง สามารถนำมาใช้ประโยชน์ เพื่อการวางแผนและตัดสินใจ และส่งผลสะท้อนไปสู่เป้าหมายหรือยุทธศาสตร์ขององค์กร

๓) กรมทางหลวง สามารถยกระดับ นำเทคโนโลยีดิจิทัลมาประยุกต์ใช้งานด้านการพัฒนาระบบทางหลวง ให้บริการที่รวดเร็วครอบคลุม และความปลอดภัยบนระบบทางหลวงอย่างบูรณาการ

๔) ผู้บริหารและบุคลากรของกรมทางหลวง มีทักษะด้าน ICT และสามารถใช้ ICT และระบบสารสนเทศให้เกิดประโยชน์ในเชิงสร้างสรรค์

วิสัยทัศน์ (Vision)

"เป็นองค์กรดิจิทัล บูรณาการและพัฒนาโครงสร้างพื้นฐานมีความมั่นคงปลอดภัยสูง เพื่อขับเคลื่อนนวัตกรรมการให้บริการสู่ระบบทางหลวงที่สะดวกปลอดภัย"

พันธกิจด้าน ICT (Mission)

๑) พัฒนาประสิทธิภาพโครงสร้างพื้นฐานที่มีสมรรถนะสูง สามารถรองรับการปฏิบัติงานและการให้บริการ

๒) พัฒนาระบบสารสนเทศเพื่อการบริหารจัดการ ภายในกรมทางหลวงให้เกิดการบูรณาการ สามารถนำมาใช้ประโยชน์เพื่อการวางแผนและตัดสินใจ อย่างมีประสิทธิภาพ

๓) รองรับการพัฒนานวัตกรรมดิจิทัลเพื่องานวิศวกรรมทางหลวง ให้เกิดการพัฒนาระบบทางหลวง ให้บริการที่รวดเร็วครอบคลุม และการยกระดับความปลอดภัยบนระบบทางหลวงอย่างบูรณาการ

๔) ส่งเสริมและสร้างมาตรฐานด้านการบูรณาการด้านสารสนเทศ เพื่อเพิ่มช่องทางการให้บริการ ภายในหน่วยงานและสังคมภายนอก อย่างมีประสิทธิภาพ ทั่วถึงและครอบคลุม

๕) พัฒนาศักยภาพทรัพยากรบุคคลรองรับการทำงานในยุคดิจิทัล เพื่อให้สามารถขับเคลื่อนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างมีประสิทธิภาพ

ยุทธศาสตร์

- ยุทธศาสตร์ที่ ๑ เสริมสร้างประสิทธิภาพโครงสร้างพื้นฐานด้าน ICT
- ยุทธศาสตร์ที่ ๒ เสริมสร้างและพัฒนาระบบสารสนเทศเพื่อการจัดการ
- ยุทธศาสตร์ที่ ๓ พัฒนานวัตกรรมดิจิทัลเพื่องานวิศวกรรมทางหลวง (Smart Highways)
- ยุทธศาสตร์ที่ ๔ เพิ่มขีดความสามารถและสร้างมาตรฐานการให้บริการด้าน ICT
- ยุทธศาสตร์ที่ ๕ เสริมสร้างศักยภาพทรัพยากรบุคคลด้าน ICT

๑.๔.๖ นโยบายกรมทางหลวง ๒๕๖๒

กรมทางหลวงเป็นหน่วยงานที่พัฒนาด้านโครงสร้างพื้นฐาน เชื่อมโยโครงข่ายระบบการคมนาคมขนส่งทั้งทางบก ทางน้ำ ทางอากาศ และทางราง สนับสนุนการขับเคลื่อนประเทศในด้านเศรษฐกิจ สังคม วัฒนธรรม เทคโนโลยี รวมถึงด้านความมั่นคงผ่านการเชื่อมโยงโครงข่ายทางหลวงที่มีอยู่ประมาณ ๑,๕๓๒ สายทาง ระยะทางรวม ๕๑,๘๔๑ กิโลเมตร ซึ่งปัจจุบันประเทศไทยมีโครงข่ายทางหลวงที่สมบูรณ์ครอบคลุมทั่วทั้งประเทศแล้ว แต่กรมทางหลวงยังต้องมีการพัฒนาอย่างต่อเนื่องเพื่อให้ทันต่อสถานการณ์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา การทำงานของกรมทางหลวงจะต้องสอดคล้อง และเชื่อมโยงกับยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ.๒๕๖๑-๒๕๘๐) ยุทธศาสตร์ของกระทรวงคมนาคมที่กำหนดยุทธศาสตร์การพัฒนาระบบคมนาคมขนส่งระยะ ๒๐ ปี (พ.ศ.๒๕๖๑-๒๕๘๐) โดยกำหนดเป็นนโยบาย เพื่อนำไปสู่การปฏิบัติที่มุ่งผลสัมฤทธิ์

นโยบายกรมทางหลวง

นโยบายกรมทางหลวง ปี ๒๕๖๒ ได้เชื่อมโยงแนวคิด และหลักปฏิบัติที่สามารถนำมาเป็นแนวทางการทำงานที่สอดคล้องกับยุทธศาสตร์ในทุก ๆ มิติ ทั้งยุทธศาสตร์ชาติ ยุทธศาสตร์กระทรวงคมนาคม นโยบายเร่งด่วนต่าง ๆ สำหรับนโยบายกรมทางหลวงจะมุ่งเน้นนโยบายหลัก ๕ ด้านคือ

- นโยบายด้านที่ ๑ พัฒนาโครงข่ายทางหลวงและทางหลวงพิเศษระหว่างเมือง
- นโยบายด้านที่ ๒ พัฒนาโครงข่ายทางหลวงเพื่อรองรับประชาคมเศรษฐกิจอาเซียน (ASEAN Economic Community: AEC)
- นโยบายด้านที่ ๓ พัฒนาและปรับปรุงประสิทธิภาพทางหลวง
- นโยบายด้านที่ ๔ พัฒนาและดูแลรักษาทางหลวงให้ได้มาตรฐานความปลอดภัยในระดับสากล
- นโยบายด้านที่ ๕ ปรับปรุงการบริหารจัดการองค์การ พัฒนาบุคลากรตอบสนองสังคมและสิ่งแวดล้อมตามหลักธรรมาภิบาลของการบริหารกิจการบ้านเมืองที่ดี (Good Governance)

๑.๕ วัตถุประสงค์ของแผนปฏิบัติการ

๑. สร้างความเชื่อมั่นให้กับบุคลากรกรมทางหลวง ได้รับการปกป้องจากภัยคุกคามทางไซเบอร์ในทุกรูปแบบ อาทิ ระบบขัดข้อง (Disruption) จารกรรมข้อมูล (Hack) การเรียกค่าไถ่ (Hijack) การเปลี่ยนแปลงข้อมูลเพื่อการหลอกลวง เผยแพร่ข้อมูลที่ไม่เป็นจริง ฯลฯ

๒. เตรียมความพร้อม อุปกรณ์ และบุคลากรในการรับมือภัยคุกคามทางไซเบอร์ ติดตามภัยคุกคามทางไซเบอร์รูปแบบใหม่

๓. กำหนดมาตรการ กลไกในการปกป้องโครงสร้างพื้นฐานสำคัญทางด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของกรมทางหลวง และตอบโต้ในภาวะฉุกเฉินเพื่อแก้ไขปัญหา

๔. ให้บุคลากรทางไซเบอร์และผู้ใช้งานทั่วไปของกรมทางหลวง ได้รับการปลูกฝังให้ตระหนักในการร่วมกันป้องกันภัยไซเบอร์ ทั้งในด้านความรับผิดชอบ จริยธรรม และมีสติในการบริโภคข้อมูล

บทที่ ๒
สถานการณ์ที่เกี่ยวข้อง

๒.๑ สถานการณ์ภายนอกประเทศ

ปัจจุบัน ประเทศต่าง ๆ ให้ความสำคัญกับการยกระดับความพร้อมรับมือกับปัญหาภัยคุกคามไซเบอร์ภายในประเทศ และพัฒนามาตรการ ซึ่งในการประเมินความพร้อมด้านไซเบอร์ ที่อ้างอิงจาก International Telecommunication Union (ITU) หรือสหภาพโทรคมนาคมระหว่างประเทศของสหประชาชาติ ผลจากการสำรวจความพร้อมของประเทศต่าง ๆ ทั่วโลก ได้ประเมินระดับความพร้อมรับมือกับปัญหาภัยคุกคามไซเบอร์โดยใช้ดัชนี Global Cybersecurity Index (GCI) จำนวน ๕ หมวด ได้แก่ กฎหมาย (Legal) เทคนิค (Technical) องค์กร (Organizational) การพัฒนาศักยภาพ (Capacity building) และความร่วมมือ (Cooperation) เพื่อการเพิ่มขีดความสามารถด้านความปลอดภัยไซเบอร์ในระดับชาติ ภูมิภาค และระดับนานาชาติ โดยใช้ค่าเป้าหมายดัชนีชี้วัดจากGlobal Cybersecurity Index - GCI

สืบเนื่องมาจาก ไซเบอร์มีอิทธิพลต่อการดำเนินชีวิตประจำวันของประชาชนอย่างหลีกเลี่ยงไม่ได้ จากหน่วยงาน International Telecommunication Union (ITU) เผยแพร่ข้อมูลจำนวนผู้ใช้อินเทอร์เน็ตทั่วโลกเพิ่มขึ้นถึงร้อยละ ๗๐ จากจำนวนผู้ใช้ ๑.๙๙๑ พันล้านคน (๒๕๕๓) เป็นจำนวนผู้ใช้ ๓.๓๘๕ พันล้านคน (๒๕๕๙)[๑] และประเทศไทยมีผู้ใช้อินเทอร์เน็ตเพิ่มมากขึ้นเกือบสองเท่าจากจำนวนผู้ใช้ ๒๗.๖๕ ล้านคน (๒๕๕๗) เป็นจำนวนผู้ใช้ ๔๓.๘๗ ล้านคน (๒๕๕๙)[๒] ในขณะเดียวกันแนวโน้มจากภัยทางไซเบอร์ทวีความรุนแรงมากขึ้น สร้างความเสียหายในวงกว้างมากขึ้นเช่นเดียวกัน เมื่อเปรียบเทียบปริมาณข้อมูลลูกค้าบริษัทชั้นนำทั่วโลกที่ถูกแฮกเกอร์เจาะเข้าถึงระบบได้สำเร็จในช่วงหลายปีที่ผ่านมาได้แก่ The Home Depot (๕๖ ล้านคน ปี ๒๐๑๖) UBER (๕๗.๖ ล้านคน ปี ๒๐๑๖) Sony PlayStation (๗๗ ล้านคน ปี ๒๐๑๑) Facebook (๘๗ ล้านคน ปี ๒๐๑๘) Target (๑๑๐ ล้านคน ปี ๒๐๑๓) Equifax (๑๔๓ ล้านคน ปี ๒๐๑๗) ebay (๑๔๕ ล้านคน ปี ๒๐๑๔) Under Armour (๑๕๐ ล้านคน ปี ๒๐๑๘) และ Yahoo (๓ พันล้านคน ปี ๒๐๑๓-๑๔)[๓] ซึ่งตัวอย่างนี้เป็นเพียงตัวอย่างหนึ่งของการเจาะระบบได้สำเร็จ ในไซเบอร์ยังมีภัยคุกคามที่อันตรายประเภทอื่น ๆ อีกมากมาย ภัยคุกคามไซเบอร์เกิดขึ้นจากหลายสาเหตุ ไม่ว่าจะเป็นแฮกเกอร์ที่ต้องการแสดงออกทางการเมือง ทำลายชื่อเสียง เรียกร้องความสนใจเพื่อกดดันให้เกิดการเปลี่ยนแปลง โดยไม่ต้องการเปิดเผยตัวตน หรือเป็นอาชญากรไซเบอร์ที่ต้องการโกงผลประโยชน์ทางการเงิน การล่อลวงหรือหลอกลวงที่นำไปสู่การละเมิดผู้อื่น หรืออาจจะเป็นผู้ไม่หวังดีที่ต้องการนำข้อมูลในหน่วยงานตนเองไปเผยแพร่ หรือการทำลายระบบเพื่อผลประโยชน์ทางการเงิน หรือการแก้แค้น และภัยคุกคามไซเบอร์ประเภทที่ร้ายแรงที่สุดอันมีรัฐอยู่เบื้องหลัง เพื่อมุ่งหวังการจารกรรม บ่อนทำลาย หรือโจมตีผลประโยชน์ทางเศรษฐกิจ การเมือง หรือทางการทหาร เป็นต้น

---

[1] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] https://www.nbtc.go.th/News/Information/รายงานข้อมูลการใช้อินเตอร์เน็ตของประเทศไทย-ปี-2559.aspx

[3] https://www.thesslstore.com/blog/2018-cybercrime-statistics/

ประเทศที่พัฒนาแล้วมีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เพื่อการบริหารจัดการองค์กรอย่างเต็มรูปแบบมักถูกโจมตีทางไซเบอร์ปรากฏเป็นข่าวอย่างต่อเนื่อง โดยการโจมตีที่สำคัญเกิดกับโครงสร้างพื้นฐานสำคัญของประเทศ และการโจมตีทางไซเบอร์จะเป็นการโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งเกิดขึ้นทั่วโลก ดังตัวอย่างเหตุการณ์การโจมตีที่สำคัญๆ ได้แก่

- มิถุนายน ๒๕๕๓ โรงไฟฟ้านิวเคลียร์อิหร่านถูกโจมตีด้วยมัลแวร์ Stuxnet ซึ่งทำลายเครื่องจักร "Centrifuges" ที่ใช้เพิ่มประสิทธิภาพของแร่ยูเรเนียม มากกว่า ๑,๐๐๐ เครื่อง และแพร่กระจายไปยังคอมพิวเตอร์จำนวนกว่า ๒๐๐,๐๐๐ เครื่อง
- กันยายน ๒๕๕๕ ปฏิบัติการ "Operation Ababil" สถาบันการเงินสำคัญของสหรัฐอเมริกา เช่น New York Stock Exchange, J.P. Morgan Chase, Bank of America และอีกหลายแห่งถูกโจมตี DDoS โดยกลุ่ม Qassam Cyber Fighters ทำให้การบริการเว็บไซต์หยุดชะงัก
- กันยายน ๒๕๕๙ แฮคเกอร์ปล่อย มัลแวร์ Mirai ใช้ช่องโหว่ในอุปกรณ์ IoT โจมตีเครื่องให้บริการชื่อโดเมน ทำให้ไม่สามารถเข้าถึงเว็บไซต์ กระทบผู้ใช้งานทั่วโลก
- กันยายน ๒๕๕๙ ธนาคารกลางบังคลาเทศ ถูกมิจฉาชีพลอบโอนเงิน สูญ ๘๑ ล้านเหรียญสหรัฐฯ
- พฤษภาคม ๒๕๖๐ มัลแวร์ WannaCry โจมตีหน่วยงานสาธารณสุขของอังกฤษ ผู้ป่วยมากกว่า ๖,๙๐๐ รายไม่สามารถรับบริการและมัลแวร์แพร่กระจายไปมากกว่า ๑๕๐ ประเทศ
- มกราคม ๒๕๖๑ ข้อมูลผู้ใช้บริการ Florida Medicaid ของสหรัฐฯ รั่วไหล ๓๐,๐๐๐ คน
- พฤศจิกายน ๒๕๖๐ บริษัท Uber ข้อมูลส่วนบุคคลของคนขับรถและผู้ใช้บริการ รั่วไหล ๕๓ ล้านคน
- มกราคม ๒๕๖๑ ระบบฐานข้อมูลประชาชนของอินเดียกว่า ๑,๐๐๐ ล้านคน ตกเป็นข่าวว่ามีช่องโหว่ให้ผู้ไม่ประสงค์ดีเข้าถึงได้โดยไม่ได้รับอนุญาต
- กรกฎาคม ๒๕๖๐ บริษัท Equifax ข้อมูลส่วนบุคคลของผู้บริโภคชาวสหรัฐฯ รั่วไหล ๑๔๕ ล้านคน

ภัยคุกคามทางไซเบอร์ไม่ได้จำกัดผลกระทบต่อกลุ่มโครงสร้างพื้นฐานทางสารสนเทศกลุ่มใดกลุ่มหนึ่งเป็นการเฉพาะ และในหลายเหตุการณ์กลุ่มโครงสร้างพื้นฐานทางสารสนเทศมีความสัมพันธ์เชื่อมโยงกันอาจจะส่งผลต่อกลุ่มโครงสร้างพื้นฐานทางสารสนเทศอื่นทำให้เกิดผลกระทบต่อความสามารถในการให้บริการในหลาย ๆ กลุ่มได้ ทั้งนี้แนวโน้มของภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่สำคัญ ๆ ในปัจจุบันได้แบ่งออกเป็น ๓ ภัย ดังนี้

๑) ภัยคุกคามทางไซเบอร์เนื่องจากอุปกรณ์เชื่อมต่ออินเทอร์เน็ตที่เพิ่มมากขึ้น (Internet connected devices) ด้วยอัตราการเติบโตของการใช้อุปกรณ์ Internet of things (IoT) ที่เพิ่มมากขึ้นอย่างรวดเร็ว โดยที่ผู้ผลิตอุปกรณ์เหล่านั้นไม่ได้ออกแบบให้มีมาตรการด้านการรักษาความมั่นคงปลอดภัยเมื่อใช้งานอุปกรณ์เหล่านั้น ทำให้อุปกรณ์ IoT ที่ผลิตและติดตั้งจำนวนมากทั่วโลกไม่มีการตรวจสอบความมั่นคงปลอดภัย ทำให้ตกเป็นเหยื่อการโจมตีจากผู้ไม่หวังดี และการควบคุมด้วย IoT Botnets นี้ ผู้ไม่หวังดีใช้เป็นเครื่องมือไปโจมตีบุคคลที่สาม โดยใช้มัลแวร์ เช่น Mirai (การโจมตีแบบ Distributed Denial of Service (DDoS)) ทำให้เกิดปริมาณข้อมูลจราจรที่ใช้โจมตีมากถึง ๑ Terabits ต่อวินาทีโดยใช้อุปกรณ์ IoT Botnets จากการใช้กล้อง CCTV และกล้องบันทึกวิดีโอส่วนตัวมากถึง ๑๕๒,๐๐๐ เครื่องและนอกจากนี้อุปกรณ์ IoT มักจะมีจุดอ่อน

ที่เป็นอุปกรณ์ที่มีราคาถูก ผลิตออกมาเป็นจำนวนมากโดยไม่ได้ออกแบบและติดตั้งมาตรการรักษาความมั่นคงปลอดภัยมาจากโรงงานผลิต ทำให้ไม่สามารถที่จะปรับปรุงหรือปิดช่องโหว่ด้านความมั่นคงปลอดภัยได้ในภายหลัง

๒) เครื่องมือโจมตีทางไซเบอร์มีจำนวนหลากหลาย สามารถหาได้ง่ายและใช้ได้ง่ายด้วย ปัจจุบันในตลาดมืดไซเบอร์มีเครื่องมือโจมตีมากมายให้เลือกซื้อได้ มีบริการจ้างแฮกเกอร์โจมตีทางไซเบอร์ มีการให้บริการพัฒนาเครื่องมือตามความต้องการของลูกค้า และมีการให้บริการหลังการขายเหมือนกับการให้บริการธุรกิจทั่วไป

๓) การโจมตีทางไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของรัฐมีแนวโน้มสูงขึ้น โดยโลกไซเบอร์มีการเชื่อมต่อถึงกันอยู่ตลอดเวลา ประเทศต่าง ๆ ไม่สามารถตัดขาดจากอินเทอร์เน็ตได้อย่างสมบูรณ์ การเข้าถึงกันได้ง่ายในโลกไซเบอร์จึงเป็นช่องทางการโจมตีต่อรัฐเพิ่มมากขึ้นด้วยที่มาจากการโจมตีของประเทศอื่นที่ไม่ใช่พันธมิตร เกิดขึ้นได้ง่ายขึ้นด้วยไม่ว่าจะเป็นการสร้างกระแสข่าวปลอมเพื่อหลอกลวง หรือสร้างความเข้าใจที่ผิด ดังเช่น เหตุการณ์การสร้างกระแสทาง Social media ในสหรัฐอเมริกาที่ส่งผลกระทบต่อผลการเลือกตั้งประธานาธิบดีเมื่อปี พ.ศ.๒๕๕๙ ซึ่งในปีเดียวกันนั้นในประเทศไทยก็มีกระแสกลุ่ม Hacktivist โจมตีหน่วยงานและเว็บไซต์ภาครัฐด้วยเทคนิค DDoS และเปลี่ยนข้อมูลหน้าเว็บไซต์ของหน่วยงานรัฐ เนื่องจากผลการตัดสินคดีฆาตกรรมที่เกาะเต่าของไทย รวมถึงเหตุการณ์ที่กลุ่ม Anonymous ประกาศแคมเปญ SingleGateway โจมตีหน่วยงานรัฐไทยเพื่อแสดงจุดยืนของตนเอง เป็นต้น

เหตุการณ์ที่กล่าวมานี้แสดงให้เห็นว่าการพัฒนาขีดความสามารถด้านไซเบอร์เป็นสิ่งจำเป็นเพื่อให้มีศักยภาพในการตอบสนอง แจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟู ปราบปราม และตอบโต้ เมื่อถูกโจมตีโดยผู้ไม่หวังดี โดยเฉพาะอย่างยิ่งโครงสร้างพื้นฐานที่สำคัญของประเทศ ต้องมีความมั่นคงปลอดภัยทั้งทางกายภาพและความมั่นคงปลอดภัยทางไซเบอร์ด้วย

๒.๒ สถานการณ์ (เฉพาะ) ภายในประเทศ

ในปี ๒๕๖๐ ITU ได้ประเมิน Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ ๒๒ จาก ๑๙๔ ประเทศ เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ ๓ รองจากสิงคโปร์ และมาเลเซียในภาพรวมนั้นไทยมีผลประเมินด้านความพร้อมในการรับมือภัยคุกคามทางเทคนิคสูง แต่ยังขาดความพร้อมด้านการจัดตั้งองค์กรและนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อีกทั้งยังขาดความร่วมมือระหว่างหน่วยงานทั้งในและต่างประเทศในการต่อต้านภัยคุกคามไซเบอร์

ดังนั้นแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยฉบับนี้จะต้องนำมาปฏิบัติเพื่อให้เกิดการยกระดับความพร้อมรับมือกับปัญหาภัยคุกคามไซเบอร์ภายในประเทศ ซึ่งแผนปฏิบัติการฯ ดังกล่าว จะประกอบด้วย กำหนดองค์กรในการบริหารจัดการ พัฒนาและสร้างศักยภาพด้านไซเบอร์ในทุกมิติ สร้างความพร้อมในการรับมือกับภัยไซเบอร์ทุกรูปแบบให้เป็นไปตามมาตรฐานสากล สร้างมาตรการ กลไกตามมาตรฐานในการปกป้องโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญ พัฒนาปรับปรุงแก้ไขกฎหมายไซเบอร์ให้ทันต่อสถานการณ์โลก สร้างความร่วมมือด้านไซเบอร์ในประเทศและต่างประเทศ และสร้างภูมิคุ้มกันและปลูกฝังให้ประชาชนได้ตระหนักรู้การป้องกันภัยไซเบอร์

๒.๒.๑ ข้อมูลสถิติภัยคุกคามทางไซเบอร์

ประเทศไทยประสบกับเหตุภัยคุกคามทางไซเบอร์ในลักษณะที่คล้ายกับต่างประเทศ จากข้อมูลสถิติที่ไทยเซิร์ต (ThaiCERT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวบรวมแสดงปริมาณและประเภทของเหตุภัยคุกคามที่ได้รับแจ้งในช่วงครึ่งแรกของปี ๒๕๖๑ พบว่าภัยคุกคามไซเบอร์ที่เกิดขึ้นมีถึง ๑,๖๙๑ ครั้ง โดยประเภทของภัยคุกคามที่เกิดขึ้นปริมาณสูง ได้แก่ Intrusion Attempts คิดเป็นร้อยละ ๒๙ Fraud คิดเป็นร้อยละ ๒๖ Intrusions คิดเป็นร้อยละ ๑๘ Malicious code คิดเป็นร้อยละ ๘ Information security ร้อยละ ๒ โดยที่เหลือเป็นภัยคุกคามด้านอื่นๆ ทั้งนี้ปริมาณของ Intrusion Attempts และ Fraud มีปริมาณสูงเกินกว่าร้อยละ ๕๐ ของภัยคุกคามประเภทอื่นๆ เมื่อเทียบสถิติการเกิดภัยคุกคามไซเบอร์ในปี พ.ศ. ๒๕๖๐ และ พ.ศ. ๒๕๖๑ แล้วพบว่าในปี พ.ศ. ๒๕๖๑ มีปริมาณลดลงจากปี ๒๕๖๐ ซึ่งเกิดขึ้นจำนวนมากถึง ๓,๒๓๗ ครั้ง อย่างไรก็ตามภัยคุกคามทางไซเบอร์ยังเกิดขึ้นอยู่ตลอดเวลา โดยจากรายงานสถิติของ ECSIRT.net พบว่า ประเทศไทยยังคงติดอยู่ในลำดับต้นๆ ของประเทศที่เกิดภัยคุกคามไซเบอร์

แนวโน้มการโจมตีทางไซเบอร์เกิดขึ้นกับหน่วยงานของรัฐและเอกชน มีรายงานเหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องตั้งแต่ปี พ.ศ. ๒๕๕๕ มีการใช้วิธีการ Phishing หลอกเอา username และ password บัญชีเงินฝาก หรือเจาะระบบเพื่อแสดงความสามารถระหว่างแฮกเกอร์กันเอง ต่อมาในช่วงปี พ.ศ. ๒๕๕๖ เริ่มเห็นการใช้วิธีการ DDoS โจมตีธุรกิจการเงินและการลงทุนมากขึ้น โดยมีการส่งอีเมลขู่โจมตีล่วงหน้าเพื่อเรียกเงินแลกกับการไม่ถูกโจมตี โดยช่วงที่เกิดการโจมตีแบบ DDoS เป็นช่วงระยะเวลาเดียวกันกับการขู่โจมตีสถาบันการเงินทั่วโลก และในปี พ.ศ. ๒๕๕๘ ที่เหนือนอกจากการโจมตีด้วยวิธีการ DDoS ที่พบมากขึ้น ยังพบการใช้มัลแวร์ทั้งในรูปแบบการกระจายมัลแวร์เพื่อเข้ารหัสลับข้อมูลในเครื่องของเหยื่อ หรือการลอบติดตั้งมัลแวร์ในตู้เอทีเอ็มเพื่อควบคุมการจ่ายเงิน และในปี พ.ศ. ๒๕๕๙ เกิดเหตุการณ์สำคัญที่ทำให้หน่วยงานรัฐและเอกชนของไทยตระหนักถึงผลกระทบของภัยคุกคามไซเบอร์มากขึ้น คือการขู่โจมตีธนาคารใหญ่ด้วยวิธีการ DDoS รวมทั้งการปล้นเงินจากตู้เอทีเอ็ม และการโจมตีบริการสำคัญของรัฐ ทำให้ไม่สามารถให้บริการได้เป็นเวลาหลายชั่วโมง

ทั้งนี้ ต้นเหตุจูงใจในการโจมตีภัยทางไซเบอร์ของประเทศไทยไม่ใช่เฉพาะผลประโยชน์ทางการเงิน แต่ยังใช้เป็นเครื่องมือในการแสดงออกของภาคประชาชน ยกตัวอย่างเช่นเหตุการณ์กลุ่ม F๕ Army ที่โจมตีเว็บไซต์ของหน่วยงานภาครัฐ เนื่องจากมีความหวาดระแวงว่ารัฐบาลจะดำเนินการในเรื่อง Single gateway เพื่อดักรับข้อมูลของประชาชนบนอินเทอร์เน็ต การกระทำดังกล่าวเป็นการแสดงออกเชิงสัญลักษณ์ซึ่งส่งผลกระทบต่อความเชื่อมั่นและความน่าเชื่อถือในการขับเคลื่อนประเทศไทยในยุคดิจิทัล

๒.๒.๒ การโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศ

การกำหนดโครงสร้างพื้นฐานสำคัญในหลายประเทศมีความแตกต่างกันตามบริบทของประเทศนั้นๆ เช่น ในสหรัฐอเมริกา กำหนดกลุ่มโครงสร้างพื้นฐานสำคัญจำนวน ๑๖ กลุ่ม ในขณะที่ประเทศอังกฤษกำหนดไว้จำนวน ๙ กลุ่ม หลายประเทศตระหนักถึงความสำคัญในการปกป้องโครงสร้างพื้นฐานสำคัญ

เนื่องจากโครงสร้างพื้นฐานสำคัญของประเทศเกิดปัญหาขึ้นไม่สามารถให้บริการได้ตามปกติจะเกิดผลกระทบในวงกว้างต่อชีวิต และทรัพย์สินซึ่งจะส่งผลต่อความปลอดภัยของประชาชนและความมั่นคงทางเศรษฐกิจ

สำหรับประเทศไทยตามพระราชกฤษฎีกาว่าด้วยวิธีการปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ได้กล่าวถึง "โครงสร้างพื้นฐานสำคัญของประเทศ" (Critical Infrastructure) ไว้ว่าบรรดาหน่วยงานหรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องต่อความมั่นคงหรือต่อสาธารณชน หรือความสงบเรียบร้อยของประเทศ ควรวางแผนการรับมือกับภัยคุกคามที่มีต่อโครงสร้างพื้นฐานสำคัญของประเทศและโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

การโจมตีต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ของประเทศไทยได้แก่ ระบบให้บริการทางการเงิน การธนาคาร สาธารณูปโภค การขนส่งและโลจิสติกส์ บริการสุขภาพ พลังงาน การสื่อสารโทรคมนาคม เป็นภัยคุกคามทางไซเบอร์ ก่อให้เกิดผลกระทบที่รุนแรงในวงกว้างและสามารถสร้างความเสียหายที่ร้ายแรงต่อเสถียรภาพทางเศรษฐกิจ สังคม และความมั่นคงของประเทศ ซึ่งอาจทำให้ประเทศสูญเสียความได้เปรียบในการแข่งขันทางการค้าในตลาดโลก ทำให้ประเทศขาดความเชื่อมั่นในสายตาประชาคมโลกหรือประชาชนทั่วไป ทำให้การปฏิบัติงานของประเทศต้องหยุดชะงัก รวมทั้งผลกระทบทางกฎหมายจะต้องมีการดำเนินการทางกฎหมาย การลงโทษผู้ก่อเหตุหรือยุยงส่งเสริมให้เกิดการกระทำความผิดทางไซเบอร์ ประเทศไทยได้ประสบกับเหตุการณ์การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญ (Critical Information: CI) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ดังนี้

- มิถุนายน ๒๕๕๕ ผู้ให้บริการชื่อโดเมนไทย (.th) ถูกเจาะระบบและแก้ไขข้อมูลที่อยู่เว็บไซต์ขององค์กรใหญ่หลายแห่ง
- กุมภาพันธ์ ๒๕๕๖ การโจมตี DDoS ตลาดหลักทรัพย์ โจมตี DDoS โดยกลุ่ม Anonymous กับเว็บไซต์ตลาดหลักทรัพย์ในอเมริกา เอเชีย รวมถึงไทย ทำให้บริการขัดข้องหลายชั่วโมง แสดงให้เห็นถึงผลกระทบด้านเศรษฐกิจ
- ตุลาคม ๒๕๕๘ ๕ ธนาคารพาณิชย์ได้รับอีเมลข่มขู่ เรียกเงินเป็น Bitcoins เพื่อแลกกับการไม่ถูกโจมตี DDoS จากกลุ่ม Armada Collective จุดเริ่มต้นการหารือของ CEO Financial Sector เพื่อรับมือปัญหา Cybersecurity
- สิงหาคม ๒๕๕๙ ATM ๒๑ ตู้ของธนาคารออมสินถูกโจมตีด้วยมัลแวร์และลอบขโมยเงิน ๑๒ ล้านบาท มัลแวร์ที่พบคล้ายกับที่ใช้โจมตี ATM ในไต้หวันในปีเดียวกัน
- ธันวาคม ๒๕๕๙ ปรากฏการณ์ทางสังคมที่แสดงออกผ่านไซเบอร์ เมื่อกลุ่ม "พลเมืองต่อต้าน Single Gateway #opsinglegateway" รณรงค์ให้มีการโจมตี DDoS กับเว็บไซต์ของหน่วยงานของรัฐ ทำให้หลายระบบสำคัญของรัฐขัดข้อง และพบการเจาะฐานข้อมูลเพื่อโจรกรรมข้อมูลมาเผยแพร่ รวมถึงใช้ปฏิบัติการข่าวสาร IO ในการลดความน่าเชื่อถือของรัฐบาล
- กรกฎาคม ๒๕๖๑ การโจรกรรมข้อมูลลูกค้าสินเชื่อที่อยู่อาศัยของธนาคารกรุงไทย และข้อมูลลูกค้าบริการหนังสือค้ำประกันของธนาคารกสิกรไทย ถึงแม้จะไม่มีมูลค่าความเสียหายเป็นตัวเลข แต่ก็สร้างความเสียหายทางชื่อเสียง และความน่าเชื่อถือของกิจการธนาคารอย่างมาก

๒.๒.๓ บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ไม่เพียงพอ

การนำแผนไปสู่การปฏิบัติจะไม่สามารถดำเนินการได้หากบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์มีไม่เพียงพอ หรือไม่มีคุณภาพ บริษัทยักษ์ใหญ่ข้ามชาติหลายแห่งได้ประเมินการขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ไปในทิศทางเดียวกัน ซึ่งถือได้ว่าเป็นปัญหาระดับโลก ในปี พ.ศ. ๒๕๕๗ มีรายงานจากบริษัท ซิสโก้ ว่าทั่วโลกขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ประมาณ ๑ ล้านคน ในปี พ.ศ. ๒๕๕๘ บริษัท ไซมานเทคทำนายว่าจะมีการขาดแคลนประมาณ ๑.๕ ล้านคน และในปี พ.ศ. ๒๕๕๙ สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA) ได้ทำนายว่าจะมีการขาดแคลนประมาณ ๒ ล้านคนล่าสุดในปี พ.ศ. ๒๕๖๐ บริษัท ไซเบอร์ซีเคียวริตี้เวนเจอร์สทำนายว่าจะมีการขาดแคลนถึง ๓.๕ ล้านคน และในปี พ.ศ. ๒๕๖๑ จากการประเมินจำนวนผู้ที่ได้รับประกาศนียบัตรวิชาชีพ CISSP (Certified Information Systems Security Professional) ซึ่งเป็นประกาศนียบัตรที่ได้รับการยอมรับทั่วโลก พบว่าประเทศไทยมีผู้ที่ได้รับประกาศนียบัตรเพียง ๒๐๔ คน น้อยกว่าสิงคโปร์ (๑,๖๖๑ คน) และมาเลเซีย (๓๐๐ คน) ดังนั้น จึงมีความจำเป็นต้องพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในประเทศอย่างเร่งด่วน เพื่อรองรับความต้องการทั้งในปัจจุบันและอนาคต

ดังนั้นการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เพียงพอต่อความต้องการเป็นเรื่องจำเป็นเร่งด่วน เพื่อพร้อมรับมือภัยคุกคามไซเบอร์ที่ทวีความรุนแรงยิ่งขึ้นในอนาคต ในทุกระดับ ตั้งแต่ระดับปฏิบัติการ จนถึงระดับผู้บริหาร ทั้งในเชิงปริมาณและเชิงคุณภาพ รวมทั้งการกำหนดนโยบายและมาตรการสนับสนุน และสร้างแรงจูงใจค่าตอบแทนพิเศษสำหรับบุคลากรด้านไซเบอร์ รวมถึงนโยบายการพัฒนาศักยภาพบุคลากรและสร้างความตระหนักให้แก่ประชาชน หลักสูตรในสถานศึกษาทุกระดับที่ได้มาตรฐานสากล

๒.๒.๔ กฎหมายไม่ครอบคลุมการดำเนินการหรือไม่สอดรับกับเทคโนโลยีที่พัฒนาอย่างรวดเร็ว

ปัจจุบันประเทศไทยมีกฎหมายหลายฉบับกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้แก่ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งกำหนดมาตรการเพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือต่อการใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งกำหนดบทลงโทษสำหรับการก่ออาชญากรรมคอมพิวเตอร์ กฎหมายดังกล่าวครอบคลุมในบางมิติของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเทคโนโลยีอินเทอร์เน็ตมีการเติบโตและมีพัฒนาอย่างรวดเร็ว กฎหมายที่ใช้ในการกำกับดูแลอาจจะไม่สามารถบังคับใช้หรือไม่สามารถกำกับดูแลกับสภาพปัญหาดังกล่าวได้ เช่น การใช้เงินสกุลดิจิทัล หรือการเข้ารหัสข้อมูลที่มีความซับซ้อน และมิได้ถูกกำหนดจากกฎหมายภายในประเทศ ทำให้ภาครัฐไม่สามารถตรวจสอบการดำเนินการภายใต้กิจกรรมดังกล่าวได้ และกฎหมายอาจจะไม่เอื้ออำนวยในการดำเนินการ กฎหมายทางด้านไซเบอร์จึงต้องมีการปรับรูปแบบให้ทันสมัยอยู่เป็นประจำ โดยปรับให้สอดรับกับเทคโนโลยีได้ทันการณ์

เนื่องจากกฎหมายไซเบอร์เป็นกลไกสำคัญในการสร้างความเชื่อมั่นให้กับระบบเศรษฐกิจและสังคมดิจิทัล ประเทศยักษ์ใหญ่อย่างสหรัฐอเมริกา จีน รวมทั้งประเทศในยุโรปและอาเซียนต่างมีกฎหมายไซเบอร์เป็นกฎหมายกลาง สำหรับประเทศไทยได้มีการเตรียมความพร้อมโดยการจัดทำกฎหมายกลางเพื่อดูแล

เรื่องความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ คือ ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ... เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งกำหนดให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐ ภาคเอกชน และภาคประชาชน ในสถานการณ์ทั่วไปหรือสถานการณ์ภัยต่อความมั่นคง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

๒.๒.๕ องค์กรกำกับดูแลด้านไซเบอร์

ในขณะที่กฎหมายการรักษาความมั่นคงปลอดภัยทางไซเบอร์อยู่ระหว่างการดำเนินการ การดูแลการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ จะอยู่ในความรับผิดชอบของหน่วยงาน ๕ หน่วย ได้แก่

๑. หน่วยงานระดับนโยบาย ได้แก่ สภาความมั่นคงแห่งชาติ (สมช.) และคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีความพร้อม สามารถปกป้อง ป้องกัน และรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนเตรียมแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพและเป็นเอกภาพ และอย่างต่อเนื่อง

๒. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สร้างความเชื่อมั่นทางด้านไซเบอร์ กำหนดนโยบาย แนวปฏิบัติ และมาตรฐานสำหรับหน่วยงานของรัฐและเอกชน ดูแลการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย มีไทยเซิร์ตที่ช่วยดูแลภัยคุกคามไซเบอร์ ตลอด ๒๔ ชั่วโมง และมีกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ที่เป็นผู้รักษากฎหมาย

๓. หน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ปัจจุบันมีหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญของประเทศ เช่น กระทรวงพลังงาน กระทรวงสาธารณสุข กระทรวงมหาดไทย ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) ที่กำกับดูแลหน่วยงานให้มีเสถียรภาพในการทำงานและการให้บริการได้อย่างต่อเนื่อง

๔. หน่วยงานรักษาความสงบเรียบร้อยภายในประเทศ เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ ตำรวจสากล (Interpol) เป็นหน่วยงานที่ทำหน้าที่ป้องปรามมิให้เกิดความไม่สงบ หรือมีการกระทำความผิดตามกฎหมาย ตลอดจนติดตามตัวผู้กระทำความผิดมาลงโทษ โดยได้มีการเตรียมพร้อมกำลังคนอย่างต่อเนื่องเพื่อรองรับภัยคุกคามไซเบอร์ที่ทวีความรุนแรงขึ้นเรื่อย ๆ

๕. หน่วยงานด้านความมั่นคง ซึ่งได้ขยายพื้นที่การรักษาความมั่นคงแห่งรัฐให้ครอบคลุมพื้นที่ไซเบอร์ (Cyberspace) ในปัจจุบันกระทรวงกลาโหม กองทัพไทย และสามเหล่าทัพ ได้ตั้งหน่วยงานเฉพาะกิจสำหรับสงครามไซเบอร์ และมีการเตรียมพร้อมด้านกำลังคน กระบวนการ และเครื่องมือแต่สิ่งที่ยังขาดคือการ

จัดตั้งองค์กรตามกฎหมายการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อรับผิดชอบในการขับเคลื่อนนโยบายความมั่นคงปลอดภัยทางไซเบอร์ไปสู่การปฏิบัติ การจัดทำแผนและนโยบายแห่งชาติ และการประสานการดำเนินการระหว่างหน่วยงานที่เกี่ยวข้องในลักษณะองค์รวมของประเทศ

๒.๒.๖ การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงผ่านสื่อสังคมออนไลน์

โลกไซเบอร์เป็นพื้นที่สาธารณะที่ให้ทุกคนมีอิสระ และเสรีภาพในการแสดงความคิดเห็น ใช้สื่อสารกัน แลกเปลี่ยนความรู้ ความคิดเห็น หรือแบ่งปันความสุข ความบันเทิง มีแพลตฟอร์มแอพพลิเคชั่น เว็บบอร์ด สื่อสังคมออนไลน์หลายรูปแบบที่เปิดให้ผู้ใช้งานแสดงความคิดเห็น เช่น Instagram, Facebook, Line, Youtube, pantip.com, sanook.com ฯลฯ ประเทศไทยมีผู้ใช้งานอินเทอร์เน็ตประมาณ ๕๗ ล้านคน มีผู้ใช้งาน Facebook จำนวน ๔๖ ล้านคน ผู้ใช้งาน Line จำนวน ๕๑ ล้านคน ดังนั้นการที่จะตรวจสอบติดตามข้อมูลที่เผยแพร่อยู่ในอินเทอร์เน็ตทั้งหมด และสื่อใหม่ (New media) มีการขยายตัวอย่างรวดเร็วและมีแนวโน้มเพิ่มมากขึ้น ๆ ถึงแม้ว่าไซเบอร์จะทำให้คนไทยสามารถเข้าถึงข้อมูลที่มีประโยชน์ได้มากขึ้นและสะดวกขึ้น แต่ไซเบอร์อาจถูกใช้เป็นช่องทางที่ผู้ไม่ประสงค์ดีสร้างความวุ่นวายปั่นป่วนให้กับสังคม เช่น การเผยแพร่ข่าวเท็จ การใส่ร้ายผู้อื่น การกระพือกระแสสังคมให้เข้าใจผิด หรือสร้างความเกลียดชัง เพื่อความสนุกสนาน ผลตอบแทนทางการเงิน หรือมีวัตถุประสงค์ร้ายแอบแฝงที่ส่งผลกระทบรุนแรงต่อความมั่นคงทางสังคม เศรษฐกิจและความมั่นคงของประเทศ ดังเช่น การเผยแพร่ข่าวลวงเกี่ยวกับการทำงานของเจ้าหน้าที่รัฐ การสร้างความตระหนักเรื่องภัยธรรมชาติที่ไม่เป็นจริงตามหลักวิชาการ และด้วยคุณลักษณะของสื่อสังคมออนไลน์ที่สามารถกระจายไปในวงกว้างอย่างรวดเร็ว ดังนั้นรัฐบาล จำเป็นต้องมาดูแลปกป้อง หรือระงับการเผยแพร่ข้อมูลอันเป็นเท็จที่อาจส่งผลกระทบต่อความมั่นคงผ่านสื่อหรือผ่านทางอินเทอร์เน็ต โดยเฉพาะสื่อสังคมออนไลน์ที่ประชากรมากกว่าครึ่งหนึ่งของประเทศใช้งานอยู่เป็นประจำ ต้องสร้างความเข้มแข็งและภูมิคุ้มกันให้กับกลุ่มผู้ใช้งานอินเทอร์เน็ตที่เป็นกลุ่มเสี่ยง โดยเฉพาะเยาวชนและเด็ก ที่ยังขาดวัยวุฒิวิจารณญาณในการรับข้อมูลข่าวสารจากสื่อสังคมออนไลน์ที่ยากต่อการพิสูจน์ความแม่นยำถูกต้อง รวมถึงแหล่งที่มาของข้อมูลและส่งเสริมการเผยแพร่ข้อมูลที่ถูกต้องให้ประชาชน

๒.๒.๗ กรอบการทำงานแบบบูรณาการของหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์เพื่อให้ทำงานได้อย่างบูรณาการและมีเอกภาพ

เนื่องจากภัยคุกคามทางไซเบอร์เป็นภัยสามารถส่งผลกระทบต่อทุกหน่วยงาน ทุกประเทศทั่วโลก โดยไม่มีพรมแดนขวางกั้น ดังนั้นประเทศไทยจำเป็นต้องกำหนดกรอบการทำงาน ที่ได้บูรณาการความร่วมมือระหว่างหน่วยงานภายในและภายนอกประเทศทั้งภาครัฐและภาคเอกชน เพื่อให้นโยบายและการปฏิบัติแบบบูรณาการร่วมกับผู้ที่มีส่วนเกี่ยวข้องทุกภาคส่วนอย่างจริงจัง เช่น การบูรณาการการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ ให้มีศูนย์กลางในการสั่งการให้ทุกหน่วยงานปฏิบัติเมื่อเกิดเหตุภัยคุกคามไซเบอร์ที่รุนแรง ให้มีการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ของประเทศในลักษณะรวมศูนย์ เพื่อให้การสั่งการไปยังหน่วยปฏิบัติในกรณีเผชิญเหตุภัยคุกคามไซเบอร์ มีประสิทธิภาพ โดยให้มีการรายงานผลการปฏิบัติงานทั้งในเชิงป้องกันและการแก้ปัญหา ตามกระบวนการที่กำหนดให้หน่วยงานต่าง ๆ ทำงานร่วมกัน มีการประสานความร่วมมือระหว่างภาครัฐและภาคเอกชนเพื่อความมั่นคงปลอดภัยทางไซเบอร์

สร้างกลไกสำหรับประสานความร่วมมือระหว่างภาครัฐ ภาคเอกชน และความมั่นคงทางทหาร ที่สะท้อนการมีความรับผิดชอบต่อสังคมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของทุกภาคส่วน ในรูปแบบการมีส่วนร่วมในกระบวนการตัดสินใจ (Multi-stakeholders) การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ การรับมือสถานการณ์ฉุกเฉิน รวมถึงการกำกับดูแลหน่วยงานตนเอง

ตัวอย่างการนำนโยบาย "ความร่วมมือภาครัฐและเอกชน" เป็นกลไกสำคัญในการบรรเทาภัยคุกคาม ที่ถูกกล่าวถึงในประเทศสหรัฐอเมริกาและสหราชอาณาจักร การเป็นหุ้นส่วนภาครัฐและเอกชนถือว่าเป็น 'รากฐานที่สำคัญ' หรือ 'ศูนย์กลาง' ของยุทธศาสตร์ด้านความปลอดภัยในโลกไซเบอร์ ความเป็นหุ้นส่วนหรือการมีส่วนร่วมในการรักษาความปลอดภัยบนโลกไซเบอร์ทั้งในระดับชาติ และระดับนานาชาติ โดยบทบาทของรัฐ และหน่วยงาน ในการรักษาความปลอดภัยไซเบอร์การเป็นหุ้นส่วนภาครัฐและภาคเอกชนในการรักษาความปลอดภัยในโลกไซเบอร์ของประเทศมีหลายแง่มุม รัฐบาลต่างๆ มีความสัมพันธ์ที่หลากหลายกับผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) บริษัท ข้อมูลข้ามชาติ (Google, Facebook ฯลฯ) บริษัท รักษาความปลอดภัยในโลกไซเบอร์เอกชน หน่วยงานส่งเสริมสิทธิมนุษยชน หน่วยงานบังคับใช้กฎหมาย และภาคประชาสังคม โดยนโยบายของประเทศสหรัฐอเมริกาได้กล่าวถึงความสัมพันธ์ระหว่างรัฐบาลและผู้ประกอบการโครงสร้างพื้นฐานที่สำคัญ เนื่องจากมีความเชื่อมโยงระหว่างผลประโยชน์ของชาติในการป้องกันโครงสร้างพื้นฐานที่สำคัญกับความมั่นคงของประเทศอย่างชัดเจน ประเทศ สหรัฐอเมริกากล่าวว่าพื้นฐานการเป็นหุ้นส่วนภาครัฐและเอกชน ตามยุทธศาสตร์การรักษาความปลอดภัยในโลกไซเบอร์แห่งชาตินั้น การปฏิบัติที่เด่นชัดคือความร่วมมือระหว่างภาครัฐและภาคเอกชนในการแบ่งปันข้อมูล เช่น การให้ข้อมูลภัยคุกคามการแจ้งเตือนโลกไซเบอร์อย่างทันท่วงที ดังนั้น การแบ่งปันข้อมูลเป็นพื้นฐานของแนวคิดของ "ความร่วมมือ" หรือ “การมีส่วนร่วม” ที่ต้องให้ความสำคัญอย่างยิ่งยวด

ดังนั้น จึงจำเป็นต้องกำหนดกรอบการทำงานที่บูรณาการความร่วมมือภาครัฐและภาคเอกชน ให้ทุกภาคส่วนมีบทบาทและส่วนร่วมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

๒.๓ สถานการณ์ (เฉพาะ) ภายในกรมทางหลวง

การตระหนักรู้เรื่องการรักษาความปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐต่าง ๆ ในปัจจุบันทุกหน่วยงานให้ความสนใจเป็นอย่างมาก เนื่องจากภัยคุกคาม (Threat) มีความรุนแรงและขยายพื้นที่เพิ่มมากขึ้น ซึ่งภัยคุกคามสามารถส่งผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่ การให้บริการประชาชน การเชื่อมโยงข้อมูลกับหน่วยงานอื่น ๆ และระบบเทคโนโลยีสารสนเทศต่าง ๆ โดยอาจเกิดการขัดข้อง ติดขัด หรือหยุดชะงักได้

ภัยคุกคาม (Threat) มีหลายประเภท หลายกลุ่ม เช่น ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยเจตนา ภัยคุกคามที่ถูกทำให้เกิดขึ้นโดยไม่เจตนา ภัยคุกคามที่เกิดจากภัยธรรมชาติ และภัยคุกคามที่เกิดจากผู้ใช้ในองค์กรเอง เป็นต้น แต่ละกลุ่มสามารถแยกออกเป็นกลุ่มย่อยตามลักษณะและพฤติกรรมการทำงานของภัยคุกคามนั้นๆ

กรมทางหลวงให้ความสำคัญอย่างมากกับระบบการรักษาความปลอดภัยทางไซเบอร์ โดยกำหนดหน่วยงานกำกับดูแลด้านความปลอดภัยทางไซเบอร์ จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดหาระบบและอุปกรณ์รักษาความปลอดภัยต่าง ๆ เพื่อป้องกันภัยคุกคาม

ต่างๆ ทั้งจากเครือข่ายภายใน (Intranet) และเครือข่ายภายนอก (Internet) ที่อาจจะเกิดขึ้นได้ตลอดเวลา เพิ่มประสิทธิภาพการทำงาน เพิ่มเสถียรภาพการให้บริการของระบบสารสนเทศ และเพิ่มความน่าเชื่อถือแก่ประชาชน

๒.๓.๑ ข้อมูลสถิติภัยคุกคามทางไซเบอร์

กรมทางหลวงมีสถิติการถูกโจมตีจากภัยคุกคามทางไซเบอร์ ระดับรุนแรง จำนวนน้อยมาก ตั้งแต่ปี ๒๕๔๗ – ๒๕๖๒ โดยมีการโจมตีระดับรุนแรงเพียง ๔ – ๕ ครั้ง ซึ่งจะเป็นภัยคุกคามประเภท Ransomware โปรแกรมขุด Bit Coin และการเจาะระบบเปลี่ยนหน้า Web Site โดยกลุ่มบุคคลปริศนาแห่งโลกไซเบอร์แอนโนนีมัส (Anonymous) เท่านั้น และการโจมตีนั้นส่วนใหญ่จะมีผลกระทบกับเครื่องของผู้ใช้งาน (Client) เท่านั้น ซึ่งส่งผลกระทบในวงจำกัด และไม่สามารถส่งผลกระทบในวงกว้างได้ เนื่องจากกรมทางหลวงมีระบบตรวจจับและกักกัน (Anti-Virus , อุปกรณ์ป้องกัน และ Policy ของเครือข่าย) ภัยคุกคามไม่ให้สามารถแพร่กระจายออกไปได้ ประเด็นสาเหตุหลักที่ทำให้กรมทางหลวงมีสถิติการถูกโจมตีน้อยมากอาจจะประกอบด้วย ๒ ประเด็น ดังนี้

๑) ระบบป้องกันความปลอดภัยสามารถป้องกันภัยคุกคามได้ดีมาก

๒) กรมทางหลวงมิใช่เป้าหมายหลักของการถูกโจมตี

๒.๓.๒ หน่วยงานกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์

จากแนวโน้มและสถิติที่เพิ่มสูงขึ้นทุกปี กรมทางหลวงเล็งเห็นและให้ความสำคัญกับปัญหาดังกล่าวทั้งในปัจจุบันและอนาคตจึงเห็นควรให้จัดตั้ง กลุ่มบริหารจัดการระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ ภายใต้การกำกับดูแลของศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง เพื่อเป็นหน่วยงานกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์โดยเฉพาะ โดยมีหน้าที่ความรับผิดชอบดังนี้

- วางแผน จัดสร้างและพัฒนาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์
- กำหนดมาตรการเพื่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์
- กำหนดข้อบังคับ ระเบียบ มาตรฐาน เพื่อให้การสื่อสารข้อมูลอิเล็กทรอนิกส์ การใช้เทคโนโลยีสารสนเทศเป็นไปอย่างมีระเบียบแบบแผน มีความปลอดภัย มีความน่าเชื่อถือ
- เฝ้าระวัง ตรวจสอบการบุกรุก การคุกคามเพื่อโจมตีหรือทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์
- ควบคุม และบริหารจัดการระบบรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์
- ศึกษา ติดตามวิวัฒนาการ การบุกรุกและคุกความนำมาวิเคราะห์ประเมินผลเพื่อปรับปรุงระบบรักษาความปลอดภัยให้ทันต่อเหตุการณ์และเทคโนโลยีที่เปลี่ยนไป
- เผยแพร่องค์ความรู้ที่เกี่ยวข้องและเป็นประโยชน์ต่อผู้ใช้งาน และประสานความร่วมมือในการรักษาความปลอดภัยของระบบสารสนเทศอย่างต่อเนื่อง

๒.๓.๓ การร่วมมือกับหน่วยงานความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ

กรมทางหลวงได้ประสานความร่วมมือกับหน่วยงานการรักษาความปลอดภัยสารสนเทศในระดับประเทศ โดยการเข้าร่วมโครงการด้านการรักษาความปลอดภัยสารสนเทศ สนับสนุนข้อมูลในการวิเคราะห์การรักษาความปลอดภัย แลกเปลี่ยนข้อมูลการโจมตีจากภัยคุกคาม และความร่วมมือต่าง ๆ เพื่อเพิ่มประสิทธิภาพการป้องกัน ความรวดเร็วของการแจ้งเตือน ตอบสนองและการจัดการกับภัยคุกคามในรูปแบบต่าง ๆ ได้ทันท่วงที ส่งผลให้มีเสถียรภาพสูง หน่วยงานความมั่นคงปลอดภัยทางไซเบอร์ที่กรมทางหลวงเข้าร่วมประกอบด้วย

- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (Ministry of Digital Economy and Society: MDES)
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (Electronic Transactions Development Agency (Public Organization): EDTA)
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (Digital Government Development Agency (Public Organization): DGA)
- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team: ThaiCERT)

๒.๓.๔ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมทางหลวงได้ดำเนินการดังนี้

- จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๖ และ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับทบทวน) พ.ศ. ๒๕๖๒ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ หรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๒.๓.๕ บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ไม่เพียงพอ

การดูแลระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศเป็นงานที่ต้องบริหารจัดการ ควบคุมวางแผน กำหนดมาตรการข้อบังคับ ระเบียบ มาตรฐาน เฝ้าระวัง วิเคราะห์ ตรวจสอบ ศึกษาติดตามวิวัฒนาการ เผยแพร่องค์ความรู้ และประสานความร่วมมือในการรักษาความปลอดภัยของระบบสารสนเทศอย่างต่อเนื่อง ปัจจุบันเจ้าหน้าที่ผู้ดูแลระบบรักษาความปลอดภัยเทคโนโลยีสารสนเทศ ของกรมทางหลวง มีทั้งหมด ๕ ท่าน และด้วยภาระหน้าที่ดังที่กล่าวมาข้างต้น จึงทำให้กรมทางหลวงยังขาดแคลนบุคลากรด้านนี้เป็นอย่างมาก โดยเฉพาะยังขาดเจ้าหน้าที่ผู้ที่ได้รับประกาศนียบัตรวิชาชีพ CISSP (Certified Information System Security Professional) ซึ่งเป็นประกาศนียบัตรมาตรฐานที่ได้รับการยอมรับทั่วโลก

ดังนั้นการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ให้เพียงพอต่อความต้องการเป็นเรื่องจำเป็นเร่งด่วนเพื่อพร้อมรับมือภัยคุกคามไซเบอร์ที่ทวีความรุนแรงยิ่งขึ้นในอนาคต ในทุกระดับ ตั้งแต่ระดับปฏิบัติการ จนถึงระดับผู้บริหาร ทั้งในเชิงปริมาณและเชิงคุณภาพ

๒.๓.๖ ระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารข้อมูลของกรมทางหลวง

ความเป็นมา

ปี พ.ศ. ๒๕๔๖- ๒๕๔๗

กรมทางหลวง ได้จัดหาระบบคอมพิวเตอร์และเครือข่ายสื่อสารข้อมูลของกรมทางหลวง (เครื่องคอมพิวเตอร์แม่ข่าย ระบบงาน เครื่องคอมพิวเตอร์ลูกข่าย และเครือข่ายสื่อสารข้อมูล) สำหรับใช้ปฏิบัติงานในหน่วยงานกรมทางหลวงทั้งส่วนกลางและในภูมิภาค จากโครงการ ฯ ดังกล่าว ระบบเครือข่ายสื่อสารข้อมูลที่เชื่อมโยงไปยัง สำนักทางหลวง เป็นเครือข่าย VPN(Virtual Private Network) ๑๒๘ Kbps แขวงการทาง สำนักงานบำรุงทาง ศูนย์สร้างทาง ศูนย์สร้างและบูรณะสะพาน รวมทั้งศูนย์พัฒนาทรัพยากรบุคคลงานทางที่ศรีราชา ส่วนบริหารเครื่องจักรกล และส่วนเครื่องจักรงานทางที่ถนนแจ้งวัฒนะ กองกำกับการตำรวจทางหลวงและสถานีตำรวจทางหลวง เป็นเครือข่าย VPN แบบ Dial – up ผ่านคู่สายโทรศัพท์ธรรมดาซึ่งมีความเร็วต่ำ (๕๖ Kbps Sharing ๔ PC) การส่งสัญญาณเครือข่ายไม่ต่อเนื่องและขาดหายเป็นบางช่วงทำให้ไม่สามารถรองรับการใช้ระบบงานต่าง ๆ ได้แก่ ระบบงานสารบรรณ ระบบจัดเก็บและเผยแพร่ข้อมูลและข่าวสาร ระบบบริหารเครื่องจักรกล การใช้บริการอินเตอร์เน็ต และยังไม่มีระบบรักษาความปลอดภัยสำหรับระบบคอมพิวเตอร์และเครือข่ายสื่อสารข้อมูล

ปี พ.ศ. ๒๕๔๘- ๒๕๕๑

กรมทางหลวงจึงได้ปรับปรุงและเพิ่มประสิทธิภาพของระบบเครือข่ายสื่อสารข้อมูล รวมทั้งเครื่องมือ อุปกรณ์ต่าง ๆ ที่ใช้ในระบบเครือข่ายสื่อสารข้อมูล เพื่อให้สามารถรองรับการใช้ระบบงาน ฯ ได้อย่างมีประสิทธิภาพ มีเสถียรภาพในการให้บริการ สะดวกรวดเร็วเพิ่มขึ้น โดยมีเครือข่ายที่เชื่อมโยงไปยังทุกสำนักทางหลวง เป็นแบบ IP VPN Leased Line ที่ความเร็ว 512 Kbps แขวงการทาง สำนักงานบำรุงทาง ศูนย์สร้างทาง ศูนย์สร้างและบูรณะสะพาน รวมทั้งศูนย์พัฒนาทรัพยากรบุคคลงานทางที่ศรีราชา และส่วนบริหารเครื่องจักรกลและส่วนเครื่องจักรงานทางที่ถนนแจ้งวัฒนะ เป็นแบบ IP VPN Leased Line หรือ ADSL ที่ความเร็ว 256 Kbps มีการเช่าบริการการใช้อินเตอร์เน็ตเป็นที่ความเร็ว 10 Mbps มีการติดตั้งระบบรักษาความปลอดภัยสำหรับระบบคอมพิวเตอร์และเครือข่ายสื่อสารข้อมูล กรมทางหลวง(ระบบ Anti-virus จำนวน 1,500 Licenses) มีอุปกรณ์คอมพิวเตอร์และเครือข่ายสื่อสารข้อมูลรวมส่วนอื่นๆ ที่เกี่ยวข้อง โดยจะต้องติดตั้งที่ห้องควบคุมคอมพิวเตอร์ กองสารสนเทศ (ขณะนั้น) และที่หน่วยงานในภูมิภาคของกรมทางหลวง ได้แก่

- เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบป้องกันไวรัสคอมพิวเตอร์
- อุปกรณ์ค้นหาเส้นทาง (Router)
- อุปกรณ์จัดการการใช้งาน Internet Bandwidth
- อุปกรณ์ Web Caching
- อุปกรณ์วิเคราะห์ตรวจสอบ Network-based IPS

ปี พ.ศ. ๒๕๕๒ – ปัจจุบัน

ในปัจจุบันกรมทางหลวง ได้ดำเนินการจัดทำโครงการระบบเครือข่ายสื่อสารข้อมูลสำรอง (Backup Link) เพื่อการเชื่อมโยงข้อมูลระหว่างกรมทางหลวงกับ หน่วยงานในภูมิภาค ทั่วประเทศ รวม ๑๓๗ หน่วยงาน เพื่อรองรับการสื่อสารข้อมูลกรณีเกิดปัญหาขัดข้องต่อระบบเครือข่ายสื่อสารข้อมูลหลัก (MOTNET) เพื่อให้การใช้ระบบสารสนเทศของ กรมทางหลวง การประชุมด้วยระบบเว็บคอนเฟอร์เรนซ์ (Web Conference) การใช้บริการระบบบริการโทรศัพท์ผ่านระบบอินเตอร์เน็ต (VoIP) สามารถทำงานผ่านระบบเครือข่ายสื่อสารข้อมูลดำเนินไปอย่างต่อเนื่อง ไม่ติดขัด มีประสิทธิภาพในการให้บริการประชาชนตลอดเวลา

จากระยะเวลาที่ผ่านมามีการพัฒนาปรับปรุงระบบเครือข่ายสื่อสารข้อมูลของกรมทางหลวงมาโดยตลอดจนในปัจจุบัน เครือข่ายที่เชื่อมโยงไปยังหน่วยงานในภูมิภาค ๑๓๗ หน่วยงาน เป็นแบบ MPLS VPN ที่ความเร็ว ๒ Mbps เครือข่ายที่ติดตั้งเชื่อมโยงเครือข่ายจากสำนักงานที่อยู่ในภูมิภาคมาที่ ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง เป็นแบบ MPLS VPN ที่ความเร็ว ๓๖ Mbps และ ๑๔ Mbps อุปกรณ์คอมพิวเตอร์และเครือข่ายสื่อสารข้อมูลส่วนอื่นๆ ที่เกี่ยวข้องที่จะต้องติดตั้ง ที่ห้องควบคุมคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศ และที่สำนักงานส่วนภูมิภาคของ กรมทางหลวง ได้แก่

- อุปกรณ์ Web Caching
- อุปกรณ์จัดการการใช้งาน Internet Bandwidth
- อุปกรณ์วิเคราะห์ตรวจสอบ Network-based IPS
- อุปกรณ์กระจายการทำงานสำหรับเครือข่าย Load Balancr
- อุปกรณ์ค้นหาเส้นทาง (Router) จำนวนรวมทั้งหมด ๑๓๗ ชุด ติดตั้งที่สำนักงานในภูมิภาค ของกรมทางหลวง

๒.๓.๗ ระบบป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ ของกรมทางหลวง

ความเป็นมา

ปี พ.ศ. ๒๕๕๐ – ๒๕๕๕

กรมทางหลวงมีการนำเทคโนโลยีสารสนเทศมาใช้ปฏิบัติงานตามภารกิจต่างๆ ภายในกรมทางหลวง จัดหาและพัฒนาระบบงานคอมพิวเตอร์ ระบบการสำรวจ การจัดเก็บและการใช้ประโยชน์ข้อมูลสารสนเทศ เพื่อการบริหาร และจัดการ รวมถึงการให้บริการอินเตอร์เน็ต โดยมีการเชื่อมโยงครือข่ายสื่อสารข้อมูลทั้งภายใน และภายนอกหน่วยงาน จากการให้บริการที่มากและหลากหลายดังกล่าว กรมทางหลวงจึงเห็นความสำคัญของความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ซึ่งในปัจจุบันมีความเสี่ยงจากการบุกรุกระบบเครือข่ายสื่อสารข้อมูล จากผู้ไม่ประสงค์ดี ด้วยวิธีการต่าง ๆ มากมาย ไม่ว่าจะเป็น แฮคเกอร์ ที่ส่งแพคเก็ตข้อมูลที่สามารถทำให้เกิดทราฟฟิกมากมายบนเครือข่าย และเสี่ยงต่อถูกคุกคามจากไวรัสคอมพิวเตอร์ซึ่งมีความร้ายแรง มีการแพร่กระจาย มีความซับซ้อนและยากต่อการตรวจจับมากขึ้น การโจมตีของไวรัสและผู้บุกรุกดังกล่าวส่งผลต่อเสถียรภาพการทำงานของระบบ ทำให้ระบบเครือข่ายล่ม หรือทำงานช้าลงได้ ซึ่งมีผลกระทบต่อการปฏิบัติงานของเจ้าหน้าที่ โดยเฉพาะอย่างยิ่งการปฏิบัติงานที่ต้องการข้อมูลเร่งด่วน ในการบริการประชาชน จึงจำเป็นต้องมีระบบป้องกันและรักษาความปลอดภัยเครือข่ายสื่อสารข้อมูล เพื่อให้ระบบ

สารสนเทศมีเสถียรภาพ เจ้าหน้าที่ของกรมทางหลวงสามารถปฏิบัติงานตามภารกิจที่ได้รับมอบหมายได้อย่างมีประสิทธิภาพ ถูกต้อง สะดวกรวดเร็วและปลอดภัย กรมทางหลวงจึงได้จัดทำโครงการติดตั้งระบบป้องกันและรักษาความปลอดภัยเครือข่ายสื่อสารข้อมูล โดยมีอุปกรณ์ป้องกันและรักษาความปลอดภัยเครือข่ายกรมทางหลวง ได้แก่

- อุปกรณ์ป้องกันการโจมตีทางเครือข่าย (Intrusion and Prevention System)
- เครื่องแม่ข่ายสำหรับระบบบริหารจัดการอุปกรณ์ป้องกันการโจมตีทางเครือข่าย
- อุปกรณ์ตรวจสอบและป้องกันไวรัส (Content Security Gateway)
- อุปกรณ์ควบคุมและตรวจจับการเข้าถึงระบบเครือข่าย (Network Access Control)
- อุปกรณ์เก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log Management)
- อุปกรณ์เครื่องแม่ข่ายสำหรับให้บริการข้อมูลบัญชีรายชื่อผู้ใช้งาน ซึ่งเทคโนโลยีในขณะนั้นสามารถทำงานได้ในระดับหนึ่ง

<u>ปี พ.ศ. ๒๕๕๖ – ปัจจุบัน</u>

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลการจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ กำหนดให้ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเตอร์เน็ต หรือให้สามารถติดต่อสื่อสารผ่านทางระบบคอมพิวเตอร์ ต้องดำเนินการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ที่สามารถระบุตัวบุคคลที่ใช้งาน การจัดเก็บข้อมูลโดยวิธีการมั่นคงปลอดภัย และสามารถกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว และตามคำรับรองการปฏิบัติราชการประจำปีงบประมาณ พ.ศ. ๒๕๕๖ ตัวชี้วัดที่ ๙ ระดับความสำเร็จของการพัฒนาปรับปรุงสารสนเทศ

เนื่องจากระบบป้องกันและรักษาความปลอดภัยเครือข่ายสื่อสารข้อมูล ที่กรมทางหลวงใช้งานอยู่เดิมเริ่มล้าสมัยไม่สามารถป้องกันและรักษาความปลอดภัยเครือข่ายได้อย่างมีประสิทธิภาพ กรมทางหลวง จึงได้ติดตั้งระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ เพื่อเพิ่มระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ โดยมีวัตถุประสงค์ ดังนี้

๑. กรมทางหลวงสามารถจัดเก็บ รวบรวม และวิเคราะห์ข้อมูลการจราจรทางคอมพิวเตอร์ (Log Consolidation) ของอุปกรณ์ภายในระบบเครือข่ายสื่อสารข้อมูลของหน่วยงานในกรมทางหลวง เพื่อใช้เป็นหลักฐานสำคัญในการวิเคราะห์หาผู้กระทำความผิดทางคอมพิวเตอร์ ซึ่งสอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒. สามารถพิสูจน์ตัวตนของผู้ใช้งานเพื่อกำหนดสิทธิ์และควบคุมการเข้าใช้งานเครือข่ายคอมพิวเตอร์ของกรมทางหลวงผ่านระบบการพิสูจน์ตัวตน (User Authentication) ได้

๓. สามารถป้องกันการโจมตีเครือข่ายภายในกรมทางหลวง เพื่อเสริมศักยภาพด้านความปลอดภัยให้กับผู้ใช้งานอินเทอร์เน็ต โดยสามารถป้องกันการโจมตีจากเครือข่ายภายนอกหรืออินเทอร์เน็ตจากผู้ไม่ประสงค์ดี เช่น Hacker หรือ Attacker รวมถึงสามารถป้องกันการแพร่ระบาดของมัลแวร์ (Malware) ต่างๆ ได้แก่ ไวรัส (Virus), เวิร์ม (Worm), Spyware และโทรจัน (Trojan) บางชนิดที่มีการแพร่กระจายจากอินเทอร์เน็ตสู่เครือข่ายภายในกรมทางหลวงได้

๔. สามารถป้องกันการโจมตีหรือแพร่ระบาดมัลแวร์ (Malware) ต่างๆ จากเครื่องคอมพิวเตอร์ภายในเครือข่ายกรมทางหลวงไปยังเครือข่ายภายนอก (Internet) เพื่อเพิ่มความน่าเชื่อถือและความไว้วางใจในการติดต่อสื่อสารกับระบบเครือข่ายกรมทางหลวงจากบุคคลภายนอก

ดังนั้นเพื่อให้ระบบรักษาความปลอดภัยเครือข่ายสื่อสารข้อมูล และระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ ของกรมทางหลวง สามารถป้องกันการบุกรุกทางเครือข่ายได้อย่างมีประสิทธิภาพ สามารถจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ได้อย่างต่อเนื่อง พร้อมใช้งานได้ดีตลอดเวลา กรมทางหลวงจึงจัดทำโครงการจ้างเหมาบำรุงรักษาระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ เพื่อเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ ซึ่งสอดคล้องตามยุทธศาสตร์ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน เป้าหมายที่ ๕ ตัวชี้วัดที่ ๕.๓ ความเสี่ยงต่อการถูกคุกคามจากอาชญากรรมคอมพิวเตอร์ และเพื่อให้สามารถดำเนินการตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ถูกต้องต่อไป

๒.๔ แนวโน้มสถานการณ์ ๕ ปี และปัญหาสำคัญที่ต้องดำเนินการ

แนวโน้มสถานการณ์ ๕ ปี และปัญหาสำคัญที่ต้องเร่งดำเนินการภายใน ๕ ปี (๒๕๖๐ – ๒๕๖๔) กรมทางหลวงมีแผนดำเนินการยกระดับมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยใช้แนวทางตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และกรอบมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นหลัก รวมถึงมาตรฐานและแนวปฏิบัติของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ ด้วย ซึ่งที่ผ่านมา กรมทางหลวงได้ปฏิบัติตามแนวทางฯ ดังกล่าว แล้ว โดยกรมทางหลวงจะเพิ่มความเข้มข้น และเคร่งครัดมากยิ่งขึ้น และได้สรุปแนวทางด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญ ๆ เพื่อเป็นแนวทางปฏิบัติไว้ดังนี้

- กำหนดและทบทวนนโยบายด้านความมั่นคงปลอดภัยขององค์กร
- จัดทำโครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ อาทิเช่น กำหนดหน้าที่ความรับผิดชอบให้ชัดเจน กำหนดนโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา การปฏิบัติงานจากระยะไกล เป็นต้น
- การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ อาทิเช่น การสรรหาบุคลากร การทำข้อกำหนดและเงื่อนไขการจ้างงาน การกำหนดหน้าที่ความรับผิดชอบของผู้บริหาร การจัดให้มีการอบรมให้ความรู้อย่างเป็นรูปธรรมและเพียงพอ เป็นต้น
- การบริหารจัดการสินทรัพย์ อาทิเช่น การจัดทำทะเบียนสินทรัพย์ การกำหนดความเป็นเจ้าของสินทรัพย์ การอนุญาตให้ใช้สินทรัพย์ เป็นต้น
- การควบคุมการเข้าถึงเครือข่าย ข้อมูลและระบบสารสนเทศ
- การเข้ารหัสข้อมูล

- ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม อาทิเช่น การกำหนดพื้นที่มั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยสำนักงาน ห้องทำงาน และเครื่องมือต่าง ๆ เป็นต้น
- ความมั่นคงปลอดภัยสำหรับการดำเนินงาน อาทิเช่น การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร การจัดการเปลี่ยนแปลง การจัดการขีดความสามารถ
- ความมั่งคงปลอดภัยสำหรับการสื่อสารข้อมูล อาทิเช่น การควบคุมการเข้าถึงเครือข่าย การใช้บริการเครือข่าย การจัดแบ่งเครือข่ายภายใน การถ่ายโอนสารสนเทศ เป็นต้น
- การจัดหา พัฒนา และดูแลระบบสารสนเทศ
- ความสัมพันธ์กับผู้ให้บริการภายนอก
- การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- การบริหาร จัดการ เพื่อสร้างความต่อเนื่องในการทำงาน
- การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษ ของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

บทที่ ๓
เป้าประสงค์แห่งความสำเร็จ

เป้าหมาย ผลลัพธ์ ตัวชี้วัด ระยะ ๒๐ ปี

เป้าหมาย	ตัวชี้วัด	ค่าเป้าหมาย			
		ปี พ.ศ. ๖๑-๖๕	ปี พ.ศ. ๖๖-๗๐	ปี พ.ศ. ๗๑-๗๕	ปี พ.ศ. ๗๖-๘๐
๑. กำหนดแนวคิดมาตรการ มาตรฐานการบริหารจัดการในการป้องกัน Cyber Security ในภาพรวม	มีนโยบายและแนวทางการปฏิบัติ Cyber Security ของกรมทางหลวงที่สอดคล้องกับประเทศ	ปี ๖๒: จัดทำเสร็จเรียบร้อย	ทบทวน	ทบทวน	ทบทวน
๒. พัฒนาระบบป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของกรมทางหลวง ให้มีความปลอดภัยตามมาตรฐานสากลด้านไซเบอร์	ร้อยละของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ที่มีการพัฒนาระบบป้องกันตามมาตรฐานสากลด้านไซเบอร์	ร้อยละ ๘๐	ร้อยละ ๑๐๐	ร้อยละ ๑๐๐	ร้อยละ ๑๐๐
๓. พัฒนาศักยภาพการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมทางหลวง ให้มีขีดความสามารถในการเฝ้าระวัง การปฏิบัติการเชิงรับ และกอบกู้ฟื้นฟู	ร้อยละของแผนงาน/โครงการ ที่ได้ดำเนินการตามแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมทางหลวง ปี พ.ศ. ๒๕๖๒	ร้อยละ ๕๐	ร้อยละ ๑๐๐	ร้อยละ ๑๐๐	ร้อยละ ๑๐๐
๔. พัฒนาการบริหารจัดการเพื่อเฝ้าระวังภัยคุกคามทางไซเบอร์ให้ได้รับความเชื่อมั่นและเป็นไปตามมาตรฐานสากล	ระดับความเชื่อมั่นในการบริหารจัดการและเฝ้าระวังภัยคุกคามทางไซเบอร์	ระดับ ๓ (พอใช้)	ระดับ ๔ (ดี)	ระดับ ๕ (ดีมาก)	ระดับ ๕ (ดีมาก)
๕. มีการป้องกันและปราบปรามการเผยแพร่ข้อมูลที่มีผลกระทบต่อความมั่นคงที่เป็นรูปธรรม	ร้อยละของจำนวนข้อมูลที่มีการดำเนินการโต้ตอบแก้ไขได้ภายในระยะเวลาไม่เกิน ๒๔ ชั่วโมง	ร้อยละ ๑๐	ร้อยละ ๒๐	ร้อยละ ๓๐	ร้อยละ ๔๐

บทที่ ๔
การดำเนินการ

๔.๑ แนวความคิดในการแก้ไขปัญหาแบบบูรณาการ (ต่อปัญหาสำคัญ)

แนวทางในการปฏิบัติเพื่อรับมือกับภัยคุกคามทางไซเบอร์จะต้องดำเนินการให้เป็นไปตามหลักมาตรฐานสากล โดยมีขั้นตอน ดังนี้

ขั้นตอนที่ ๑ การเตรียมการ

ความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ประกอบด้วย หน่วยงานที่รับผิดชอบ มาตรการป้องกัน เครื่องมือและบุคลากร แผนฉุกเฉิน แผนสำรองข้อมูล

๑. กรมทางหลวงกำหนดภารกิจให้ ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้ดูแลเทคโนโลยีสารสนเทศของกรมทางหลวง รวมทั้งบริหารจัดการ มาตรการ/มาตรฐาน แนวทางที่กำหนด (Identify, Protect, Detect, Respond, Recovery) ติดตามและประเมินผลดำเนินการ และนำนโยบายไปสู่แนวปฏิบัติ

- Identify การระบุและเข้าใจเพื่อการบริหารจัดการความเสี่ยงภัยคุกคามทางไซเบอร์
- Protect การวางมาตรฐานควบคุมเพื่อปกป้องระบบเทคโนโลยีสารสนเทศ
- Detect การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ผิดปกติที่เกิดขึ้น
- Respond การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น
- Recovery การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจดำเนินการได้อย่างต่อเนื่องและฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

๒. ปรับปรุงแก้ไข ทบทวน นโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ และมาตรการต่าง ๆ ที่เกี่ยวข้อง เพื่อให้ทันต่อความก้าวหน้าและการเปลี่ยนแปลงของเทคโนโลยีดิจิทัล และสอดคล้องกับแนวปฏิบัติตามมาตรฐานสากล

๓. มาตรการป้องกัน ให้จัดทำมาตรการป้องกันภัยทางไซเบอร์ มาตรการรับมือ ต้องมีมาตรฐานความปลอดภัยของข้อมูล จัดทำมาตรฐานให้ทุกหน่วยงาน ตั้งแต่ระดับหน่วยงานระดับปฏิบัติการจนถึงหน่วยงานที่มีหน้าที่กำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๔. เครื่องมือและบุคลากร จัดให้มีอุปกรณ์และเครื่องมือเทคโนโลยีพร้อมรับมือภัยคุกคามต่าง ๆ ได้แก่ ช่วย แจ้งเตือน ป้องปราม ป้องกัน แก้ไข และฟื้นฟู และปราบปราม/ตอบโต้ และพัฒนาบุคลากรระดับ (ปฏิบัติการ/เชี่ยวชาญ/บริหาร) มีการจัดฝึกอบรมทุกระดับ

๕. แผนฉุกเฉิน ให้จัดทำรายละเอียดแผนฉุกเฉินเพื่อเตรียมความพร้อมกับสถานการณ์ที่เกิดขึ้นจริงในกรมทางหลวงและภายนอกกรมทางหลวง โดยให้หน่วยงานจัดทำแผนสำรองและกู้คืนข้อมูล และฟื้นฟูระบบและในยามปกติ ให้มีการซักซ้อมการรับมือ แลกเปลี่ยนข้อมูล รวมถึงงานข่าว และข่าวกรองทางไซเบอร์เพื่อเตรียมความพร้อมรับมือในภาวะวิกฤต

ขั้นตอนที่ ๒ การรับมือเมื่อเกิดเหตุ

แนวทางการปฏิบัติการรับมือภัยคุกคามทางไซเบอร์ (หยุดการกระทำ) จะต้องดำเนินการปฏิบัติการรับมือภัยคุกคามโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ได้จัดลำดับเป็น ๒ ระดับ ดังนี้

๑. เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบในระดับหน่วยงานย่อย บริหารจัดการโดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๒. เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อกรมทางหลวง บริหารจัดการโดยผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

สถานการณ์ด้านไซเบอร์ทั้งจากภายในและภายนอกกรมทางหลวง ทำให้เห็นได้ว่า การก้าวสู่สังคมดิจิทัลนั้น ควรมีการปกป้องบริการที่สำคัญจากภัยคุกคาม การสร้างความมั่นคงปลอดภัยทางไซเบอร์ กรมทางหลวง จึงได้กำหนดกลยุทธ์เพื่อขับเคลื่อนในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ โดยประกอบด้วย ๘ กลยุทธ์ ดังนี้

กลยุทธ์ที่ ๑) กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม

กลยุทธ์ที่ ๒) จัดองค์กรโครงสร้าง อำนาจ หน้าที่ ขีดความสามารถในงานความมั่นคงปลอดภัยทางไซเบอร์

กลยุทธ์ที่ ๓) กำหนดระบบบริหารจัดการในแต่ละระดับชัดเจน

กลยุทธ์ที่ ๔) สร้างระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน

กลยุทธ์ที่ ๕) ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ ๖) ป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

กลยุทธ์ที่ ๗) สร้างความตระหนักรู้ให้บุคลากรของหน่วยงาน

กลยุทธ์ที่ ๘) พัฒนาศักยภาพเทคโนโลยีและบุคลากร

๔.๒ กลยุทธ์

กลยุทธ์ที่ ๑ กำหนดแนวความคิด, มาตรการ, มาตรฐาน, ระบบบริหารจัดการในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อนำมาใช้เป็นมาตรการ มาตรฐาน ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (เดิม) ได้มีมติในการประชุมของคณะกรรมการฯ วันที่ ๒๖ ธันวาคม ๒๕๕๕ เห็นชอบต่อนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรมทางหลวงได้นำมาประกาศใช้ ในวันที่ ๓๐ มกราคม ๒๕๕๖

ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้มีความสมบูรณ์ครบถ้วน ตามเจตนาที่กฎหมายกำหนดไว้ ซึ่งอยู่ขั้นตอนการพิจารณาจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

บริหารจัดการ นโยบาย มาตรการ มาตรฐาน และความร่วมมือทุกภาคส่วนทั้งภายในส่วนกลางและภูมิภาค กรมทางหลวง โดยกำหนดกรอบแนวคิดด้านไซเบอร์ แนวทางการติดตามและประเมินผล กรอบการปรับปรุงให้ทันต่อสภาพแวดล้อมและสถานการณ์ด้านไซเบอร์ที่อาจเปลี่ยนไป ส่งเสริมสนับสนุนให้บุคลากรมีส่วนร่วมและให้ความร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์ภายในกรมทางหลวง

(๑) การบูรณาการการจัดการความมั่นคงปลอดภัยทางไซเบอร์

(๒) การสร้างมาตรการ กลไก ระเบียบและแนวทางปฏิบัติเพื่อพัฒนาศักยภาพการตอบสนองต่อภัยคุกคามไซเบอร์

(๓) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๔) การพัฒนาระบบเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

(๕) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์

(๖) การสร้างความตระหนักและความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

กลยุทธ์ที่ ๒ การจัดองค์กร โครงสร้าง อำนาจหน้าที่ ขีดความสามารถในงานความมั่นคงปลอดภัยทางไซเบอร์

กรมทางหลวง มีศูนย์เทคโนโลยีสารสนเทศ เป็นหน่วยงานหลักที่ทำหน้าที่รับผิดชอบในการบริหารจัดการและดูแลให้บริการงานด้านเทคโนโลยีสารสนเทศ โดยมีโครงสร้างดังนี้

โดยกลุ่มบริหารจัดการระบบความปลอดภัยเทคโนโลยีสารสนเทศทำหน้าที่ดูแลงานด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศทั้งส่วนกลางและในภูมิภาคครอบคลุมทั่วประเทศ มีหน้าที่ดังนี้

(๑) วางแผน จัดสร้างและพัฒนาระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์

(๒) กำหนดมาตรการการเพื่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์

(๓) กำหนดข้อบังคับ ระเบียบ มาตรฐาน เพื่อให้การสื่อสารข้อมูลอิเล็กทรอนิกส์ การใช้เทคโนโลยีสารสนเทศเป็นไปอย่างมีระเบียบแบบแผน มีความปลอดภัย มีความหน้าเชื่อถือ

(๔) เฝ้าระวัง ตรวจสอบการบุกรุก การคุกคามเพื่อโจมตีหรือทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์

(๕) ควบคุมและบริหารจัดการระบบรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายคอมพิวเตอร์

(๖) ศึกษา ติดตามการวิวัฒนาการ การบุกรุกและคุกคาม นำมาวิเคราะห์และประเมินผล เพื่อปรับปรุงระบบรักษาความปลอดภัยให้ทันต่อเหตุการณ์และเทคโนโลยีที่เปลี่ยนไป

(๗) เผยแพร่องค์ความรู้ที่เกี่ยวข้องและเป็นประโยชน์ต่อผู้ใช้และประสานความร่วมมือในการรักษาความปลอดภัยของระบบสารสนเทศอย่างต่อเนื่อง

กลยุทธ์ที่ ๓ กำหนดระบบบริหารจัดการในแต่ละระดับชัดเจน

กำหนดการบริหารจัดการและแนวปฏิบัติร่วมให้เป็นไปตามมาตรฐานสากล เพื่อเตรียมรับมือความเสี่ยงและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่ครอบคลุม สภาวะปกติ และสภาวะที่เกิดภัยคุกคามไซเบอร์แบ่งเป็น ๒ ระดับได้แก่

(๑) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบในระดับหน่วยงานย่อย บริหารจัดการโดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๒) เหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อกรมทางหลวง บริหารจัดการโดยผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO)

โดยจะต้องสร้างความรับรู้ความเข้าใจกับหน่วยงานส่วนกลางและภูมิภาค ที่มีความเกี่ยวข้องหากถูกโจมตีและกระทบต่อความมั่นคง ให้รับรู้รับทราบถึงแนวทางปฏิบัติ แนวทางการแก้ไขปัญหาตลอดจนการตอบโต้หรือฟื้นฟู ในกรณีที่มีเป็นปัญหารุนแรง มีการซ้อมรับมือภัยคุกคามจากการจำลองสถานการณ์ที่อาจเกิดขึ้นจริงจากตัวอย่างในอดีต หรือปัญหาไซเบอร์ที่อาจจะเกิดขึ้นในอนาคต เพื่อให้สามารถรับมือต่อสถานการณ์ที่อาจเกิดขึ้นเสมือนจริง รวมทั้งต้องพัฒนาระบบสำรองของกรมทางหลวง (DR-Site) เพื่อให้ระบบและบริการที่สำคัญสามารถให้บริการได้อย่างต่อเนื่อง

ทั้งนี้กรอบมาตรฐานสำหรับแนวปฏิบัตินั้นตั้งอยู่บนพื้นฐานของหลักการบริหารความเสี่ยง และมีองค์ประกอบต่อไปนี้เป็นอย่างน้อย

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นกับระบบ ทรัพย์สิน ข้อมูล และอื่น ๆ

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามไซเบอร์

กลยุทธ์ที่ ๔ ระบบการตอบโต้ต่อสถานการณ์ฉุกเฉิน

ส่งเสริมการพัฒนากลไกในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เหมาะสมกับระดับความรุนแรงและผลกระทบที่อาจเกิดขึ้น เพื่อให้การบริหารจัดการ การสั่งการ และการรายงาน รวมถึงการแจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟู ปราบปรามปัญหาภัยคุกคามทางไซเบอร์ในสภาวะปกติ และสภาวะไม่ปกติ มีกลุ่มบริหารจัดการระบบความปลอดภัยเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบหลัก มีความรวดเร็ว ประสิทธิภาพ และมีกลไกสนับสนุนการดำเนินการที่ชัดเจน และมีแผนเผชิญเหตุภัยคุกคามที่ครอบคลุมความเสี่ยงทางไซเบอร์ของกรมทางหลวง ที่ระบุแนวทางปฏิบัติก่อนเกิดเหตุ การวิเคราะห์/ประเมินเบื้องต้น การรายงานเหตุภัยคุกคามต่อระดับนโยบาย และการยืนยันผลวิเคราะห์และประเมินผลตามลำดับ

กลยุทธ์ที่ ๕ ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

จัดทำแผนการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบเทคโนโลยีสารสนเทศ และแผนรองรับสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมทางหลวง เพื่อให้หน่วยงาน มีความพร้อม สามารถป้องกันและตอบสนองต่อปัญหาได้ นอกจากนี้ก็จะต้องฝึกซ้อมรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ รวมทั้งต้องมีการตรวจสอบและประเมินระดับความพร้อมขอหน่วยงานส่วนกลางและภูมิภาคให้อยู่ในระดับความมั่นคงปลอดภัยที่เป็นไปตามมาตรฐานสากล

กลยุทธ์ที่ ๖ ป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

ติดตั้งระบบเครือข่ายคอมพิวเตอร์ เพื่อการเชื่อมโยงข้อมูลระหว่าง หน่วยงานส่วนกลางและภูมิภาค จำนวน ๑๓๗ หน่วยงาน โดยมีศูนย์เทคโนโลยีสารสนเทศ เป็นผู้ดูแลระบบเครือข่ายทั้งหน่วยงานส่วนกลางและภูมิภาคครอบคลุมทั่วประเทศ

นำระบบพิสูจน์ตัวตน (Authentication) เข้ามาใช้งาน ซึ่งกระบวนการพิสูจน์ตัวตน ในระบบเครือข่ายสื่อสารข้อมูล ของกรมทางหลวงนั้น ผู้ใช้งานจำเป็นต้องมีบัญชีรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อทำการพิสูจน์ตัวตน สามารถเก็บรักษาข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติม ฯ ที่กำหนดไว้ โดยการนำระบบพิสูจน์ตัวตน (Authentication) เข้ามาใช้งานในกรมทางหลวงช่วยให้สามารถระบุตัวตนของผู้ใช้งานได้ ซึ่งทำให้กรมทางหลวงสามารถป้องกัน แก้ไข ปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงได้

ส่งเสริมวัฒนธรรมการใช้อินเทอร์เน็ตสร้างสรรค์และรับผิดชอบทั้งในระดับบุคคลและองค์กร มีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์ และไม่ละเมิดกฎหมาย ส่งเสริมการใช้เทคโนโลยีสารสนเทศและการสื่อสารของบุคลากร โดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกันเพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบาย รวมถึงการมีส่วนร่วมในการสะท้อนปัญหา ประเมินผลการดำเนินนโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีความพร้อมรับมือภัยคุกคามทางไซเบอร์ทั้งในรูปแบบเดิมและภัยคุกคามในรูปแบบใหม่ๆ

กลยุทธ์ที่ ๗ สร้างความตระหนักรู้ให้บุคลากรของหน่วยงาน

ส่งเสริมให้กับบุคลากรทั้งส่วนกลางและภูมิภาค มีความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์ สร้างวัฒนธรรมการมีคุณธรรมและจริยธรรมในการใช้ไซเบอร์อย่างถูกต้องและสร้างสรรค์ มีความรับผิดชอบและมีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนไซเบอร์ ไม่ละเมิดกฎหมาย สร้างความตระหนักรู้อย่างเป็นระบบและต่อเนื่อง เช่น การเผยแพร่ความรู้ต่าง ๆ ของกรมทางหลวง รวมถึงความรู้ด้านความมั่นคงปลอดภัย โดยจะจัดที่กรมทางหลวงส่วนกลาง และให้เจ้าหน้าที่จากหน่วยงานทั่วประเทศเดินทางเข้ามาร่วมงาน และเผยแพร่ความรู้เทคโนโลยีสารสนเทศโดยเฉพาะ รวมถึงความรู้ด้านความมั่นคงปลอดภัย โดยให้วิทยากรออกไปให้ความรู้แก่เจ้าหน้าที่ถึงที่ปฏิบัติงานในสำนักงานทางหลวงที่ต้นเองสังกัด

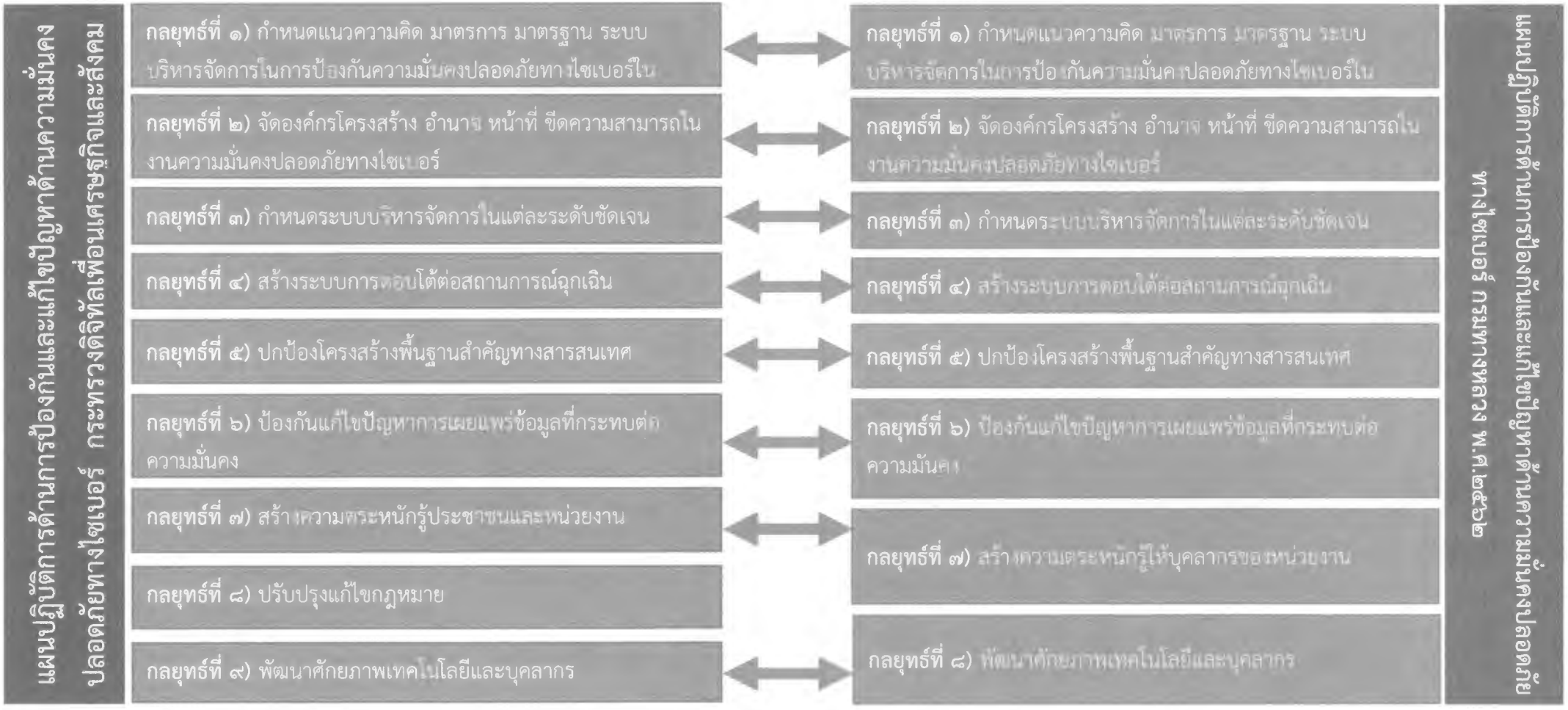
กลยุทธ์ที่ ๘ การพัฒนาศักยภาพบุคลากรและเทคโนโลยี

พัฒนาศักยภาพด้านเทคโนโลยีสารสนเทศ ให้สามารถสนับสนุนการดำเนินการใช้เทคโนโลยีสารสนเทศและการสื่อสาร สำหรับการปฏิบัติภารกิจของบุคลากรของหน่วยงานอย่างมีประสิทธิภาพ รองรับการขยายตัวของการใช้เทคโนโลยีสารสนเทศของกรมทางหลวง ทั้งในระดับบริหารและปฏิบัติงาน ให้มีความรู้ความเข้าใจและวิสัยทัศน์ในการปรับเปลี่ยนกรมทางหลวงไปสู่การเป็นรัฐบาลดิจิทัล

มีความรู้เบื้องต้นเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัล แนวโน้ม (Trend) และการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศและการสื่อสาร ความสำคัญของการใช้เทคโนโลยีดิจิทัลเพื่อเพิ่มประสิทธิภาพการทำงาน การสร้างความตระหนักรู้และการปรับตัวสู่รัฐบาลดิจิทัล

ในการเตรียมพร้อมเพื่อปรับเปลี่ยนกรมทางหลวงไปสู่การเป็นรัฐบาลดิจิทัลนั้น จะต้องพัฒนาศักยภาพของบุคลากรกรมทางหลวงในระดับต่าง ๆ ทั้งส่วนกลางและในภูมิภาค ให้มีความรู้ ความสามารถตลอดจนทักษะในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพ เท่าทันการเปลี่ยนแปลงของเทคโนโลยี มีการวางแผนฝึกอบรม เช่น การจัดหลักสูตรอบรม หรือสัมมนา เพื่อสร้างความตระหนักรู้ และเพื่อเพิ่มพูนความรู้และทักษะด้านดิจิทัลให้กับบุคลากร การปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยในการใช้งานอินเตอร์เน็ตและ เทคโนโลยีดิจิทัล การรู้เท่าทันข้อมูลเท็จในเครือข่ายสังคมออนไลน์การใช้เครือข่ายสังคมออนไลน์อย่างถูกต้องตามหลักความปลอดภัย ความรู้พื้นฐานเรื่องความมั่นคงปลอดภัย ภัยคุกคามรูปแบบต่าง ๆ การป้องกันและจัดการภัยคุกคาม ความรู้เรื่องกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติลิขสิทธิ์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เป็นต้น

แผนภาพการเชื่อมโยง กลยุทธ์แผนปฏิบัติการป้องกันแผนปฏิบัติการด้านการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ กรมทางหลวง และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



๔.๓ แผนงาน/โครงการที่สำคัญ

๔.๓.๑ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๑

๑) แผนงานพัฒนาแนวความคิด มาตรการ มาตรฐานการบริหารจัดการในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์

๑.๑) โครงการทบทวนนโยบายและแนวทางปฏิบัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรมทางหลวง

- สาระสำคัญ : เพื่อทบทวนแผน นโยบาย กรอบโครงสร้าง และระบบการบริหารจัดการแบบบูรณาการภายในกรมทางหลวง ให้ทันสมัยต่อสถานการณ์และเป็นไปตามมาตรฐานสากล
- งบประมาณ : -
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๒, พ.ศ.๒๕๖๔, พ.ศ.๒๕๖๖, พ.ศ.๒๕๖๘, พ.ศ.๒๕๗๐
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

๑.๒) โครงการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของกรมทางหลวง

- สาระสำคัญ : เพื่อจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของกรมทางหลวง
- งบประมาณ : -
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๓
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของกรมทางหลวง

๔.๓.๒ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๒

๑) แผนงานจัดตั้งองค์กร และพัฒนาขีดความสามารถในงานมั่นคงปลอดภัยไซเบอร์

- ไม่มี -

๔.๓.๓ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๓

๑) แผนงานพัฒนาศักยภาพระบบบริหารจัดการด้านไซเบอร์

๑.๑) โครงการจัดจ้างติดตั้งระบบรักษาความปลอดภัยบน Cloud Computing

- สาระสำคัญ : เพื่อจัดหาระบบบริหารจัดการงานด้านไซเบอร์ให้มีประสิทธิภาพในการเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์ กำหนดแนวทางการประสานการดำเนินงานหน่วยงานที่เกี่ยวข้องเมื่อเกิดภัยคุกคามทางไซเบอร์ และรวบรวมข้อมูลที่จำเป็น ได้แก่ บุคลากร เครื่องมือ และระบบสำรองดิจิทัล/อนาล็อก เพื่อใช้ในกิจการและการตอบโต้งานด้านความมั่นคงปลอดภัยทางไซเบอร์
- งบประมาณ : ๘,๐๐๐,๐๐๐ บาท
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๔
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

๔.๓.๔ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๔

๑) แผนงานพัฒนาศักยภาพระบบตอบโต้สถานการณ์ฉุกเฉิน

๑.๑) โครงการจัดทำแผนฉุกเฉินด้านภัยคุกคามไซเบอร์ กรมทางหลวง

- สาระสำคัญ : เพื่อจัดทำแผนฉุกเฉินโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) เพื่อค้นหาความเสี่ยงทางไซเบอร์และพัฒนาระบบป้องกันให้เป็นมาตรฐาน รวมถึงการพัฒนาศักยภาพของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ให้มีแนวทางที่ชัดเจนและสามารถปฏิบัติได้ จัดให้มีกลไกการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยทางไซเบอร์ แจ้งเตือน ป้องปราม ป้องกัน แก้ไข ฟื้นฟู และปราบปราม/ตอบโต้ ให้มีแผนเผชิญเหตุภัยคุกคามทางไซเบอร์ จัดให้มีแผนสำรองข้อมูลและอุปกรณ์รักษาความมั่นคงปลอดภัยสำหรับระบบคอมพิวเตอร์และเครือข่าย เพื่อการกู้คืนเมื่อเกิดเหตุฉุกเฉิน มีแผนสนับสนุนระบบ ฝึกซ้อมรับมือภัยคุกคามและสถานการณ์ฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมทางหลวง ในยามปกติจนถึงยามฉุกเฉินให้บูรณาการและบริหารจัดการทรัพยากร พัฒนาขีดความสามารถในการปฏิบัติการไซเบอร์เชิงป้องปรามและป้องกัน แก้ไขปัญหา ภัยคุกคามทางไซเบอร์ พัฒนาบุคลากรและแลกเปลี่ยนความรู้ องค์ความรู้
- งบประมาณ : -
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๓, พ.ศ.๒๕๖๕, พ.ศ.๒๕๖๗, พ.ศ.๒๕๖๙, พ.ศ.๒๕๗๑
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

๑.๒) โครงการเช่าบริการดาต้าเซ็นเตอร์สำรองเพื่อการกู้คืนข้อมูลกรณีเกิดภัยพิบัติ (DR site)

- สาระสำคัญ : เพื่อให้มีระบบสำรองข้อมูลที่มีเสถียรภาพและกู้คืนข้อมูลได้ เพื่อให้เกิดความมั่นใจในการใช้งานระบบงานสารสนเทศขององค์กร เพื่อให้มีศูนย์ข้อมูลสำรอง (Disaster Recover Data Center : DR DC) รองรับการเกิดภัยพิบัติที่ศูนย์ข้อมูลหลัก (Main Data Center)
- งบประมาณ : ๕,๐๐๐,๐๐๐ บาท/ปี
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๔-๒๕๗๑
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

๔.๓.๕ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๕

๑) แผนงานการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๑) โครงการจ้างเหมาบำรุงรักษาระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ เพื่อเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์

- สาระสำคัญ : เพื่อบำรุงรักษา ซ่อมแซม แก้ไข ระบบจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ และระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ ให้สามารถทำงานงานได้อย่างต่อเนื่องและมีประสิทธิภาพ ตรวจสอบ และระบุตัวตนของผู้ใช้งานผ่านระบบเครือข่ายสื่อสารข้อมูลภายในกรมทางหลวงได้ รวมทั้งมีการอัพเดทข้อมูลรูปแบบภัยคุกคาม ใหม่ๆ เพื่อป้องกันได้ทันสมัย เช่น Anti-Virus, Anti-Spam, IPS, Web filtering และ Application control ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐แก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
- งบประมาณ : ๑๕,๘๐๐,๐๐๐ บาท/ปี
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๓-๒๕๖๕, พ.ศ.๒๕๖๙-๒๕๗๑
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

๔.๓.๖ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๖

๑) แผนงานป้องกัน แก้ไขปัญหา การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

๑.๑) โครงการพัฒนาระบบบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

- สาระสำคัญ : เพื่อพัฒนาระบบบริหารจัดการและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
- งบประมาณ : ๗๐ ล้านบาท
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๖-๒๕๖๗
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ กรมทางหลวง

๔.๓.๗ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๗

๑) แผนงานการสร้างความตระหนักรู้แก่บุคลากร

๑.๑) โครงการสร้างความตระหนักรู้ การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยทางไซเบอร์

- สาระสำคัญ : เพื่อสร้างความตระหนักรู้แก่บุคลากร กรมทางหลวง ด้านความมั่นคงปลอดภัยทางไซเบอร์ และภัยคุกคามทางไซเบอร์
- งบประมาณ : ๕๐๐,๐๐๐ บาท/ปี
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๒, พ.ศ.๒๕๖๔, พ.ศ.๒๕๖๖, พ.ศ.๒๕๖๘, พ.ศ.๒๕๗๐
- หน่วยงานดำเนินการที่สำคัญ : ศูนย์เทคโนโลยีสารสนเทศ

๔.๓.๘ แผนงานโครงการสำคัญสนับสนุนกลยุทธ์ที่ ๘

๑) แผนงานพัฒนาศักยภาพบุคลากรของหน่วยงาน

๑.๑) โครงการพัฒนาศักยภาพบุคคลากรด้านไซเบอร์ (มาตรฐานด้านความปลอดภัย ISO, CAS STAR ,NIST ,EU General Protection Regulation (GDPR))

- สาระสำคัญ : พัฒนาศักยภาพบุคคลากรภาครัฐด้านไซเบอร์ เพื่อปกป้อง ป้องกัน และแก้ไขปัญหาภัยคุกคามทางไซเบอร์ จำนวน ๑๐ ท่าน
- งบประมาณ : ๑,๐๐๐,๐๐๐ บาท
- ระยะเวลาดำเนินการ : พ.ศ.๒๕๖๔
- หน่วยงานดำเนินการที่สำคัญ : ผู้ให้อบรมด้านมาตรฐานความปลอดภัยด้านสารสนเทศ

บทที่ ๕
การขับเคลื่อนและติดตามประเมินผล

๕.๑ แนวทางการขับเคลื่อนแผนฯ สู่การปฏิบัติ

ให้กลุ่มบริหารจัดการระบบความปลอดภัยเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ดำเนินการตามแผนฯ และมีการติดตามประเมินผลอย่างต่อเนื่อง

๕.๒ แนวทางการติดตามและประเมินผล

๕.๒.๑ มีกลุ่มบริหารจัดการระบบความปลอดภัยเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่กำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ ของกรมทางหลวง เพื่อวางนโยบาย และกำหนดหน่วยงานปฏิบัติ และติดตามประเมินผลโดยเฉพาะ

๕.๒.๒ กำหนดเป็นตัวชี้วัดของศูนย์เทคโนโลยีสารสนเทศ ในการกำกับ ดูแล สนับสนุน ส่งเสริมการบริหารจัดการ และการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมทางหลวง

๕.๓ กลไกแห่งความสำเร็จ

๕.๓.๑ กรมทางหลวงต้องให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และผลักดันให้เกิดผล เป็นรูปธรรม ชัดเจน และต่อเนื่อง

๕.๓.๒ กลุ่มบริหารจัดการระบบความปลอดภัยเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่กำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อวางนโยบาย และปฏิบัติงานอย่างชัดเจน

๕.๓.๓ หน่วยงานภายในกรมทางหลวง ต้องปฏิบัติตามแนวทางกลยุทธ์ของแผนปฏิบัติการฉบับนี้ และดำเนินการตามแผนปฏิบัติงานอย่างจริงจัง

๕.๓.๔ หน่วยงานภายในกรมทางหลวงต้องให้ความร่วมมือ และมีส่วนร่วมในการดำเนินงานตลอดจนร่วมกันสร้างความตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๕.๓.๕ ต้องมีการทบทวนประเมินผลการปฏิบัติการของแผนอย่างน้อยปีละ ๑ ครั้ง เพื่อปรับปรุงให้เป็นปัจจุบันและทันสมัยอย่างสม่ำเสมอ