

สำเนา

ด่วนที่สุด

ที่ นร ๐๕๐๕/ว ๙๕๙

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๕ กันยายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

กราบเรียน/เรียน รอง-นรม., รัฐ-นร., กระทรวง, กรม

สิ่งที่ส่งมาด้วย บัญชีสำเนาหนังสือที่ส่งมาด้วย

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ไปเพื่อดำเนินการ ซึ่งหน่วยงานที่เกี่ยวข้องได้เสนอความเห็นและข้อเสนอแนะไปเพื่อประกอบการพิจารณาของคณะรัฐมนตรีด้วย ความละเอียดปรากฏตามบัญชีสำเนาหนังสือที่ส่งมาด้วยนี้

คณะรัฐมนตรีได้ประชุมปรึกษาเมื่อวันที่ ๒ กันยายน ๒๕๖๘ ลงมติว่า

๑. เห็นชอบและอนุมัติตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ และให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานที่เกี่ยวข้องรับความเห็นและข้อเสนอแนะของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักเลขาธิการนายกรัฐมนตรี สำนักงบประมาณ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ และสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ไปพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

๒. ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดให้มีกิจกรรมหรือการดำเนินงานเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ เช่น การให้บริการตรวจค้นหาช่องโหว่หรือการทดสอบเจาะระบบแก่ระบบสารสนเทศก่อนนำไปใช้งานจริงโดยไม่มีค่าใช้จ่าย การเป็นหน่วยงานกลางในการจัดฝึกอบรมผู้พัฒนาระบบและบุคลากรที่เกี่ยวข้อง รวมถึงสนับสนุนการเฝ้าระวังภัยคุกคามทางไซเบอร์ให้แก่ระบบสารสนเทศของหน่วยงานของรัฐทั้งหมด เพื่อป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

จึงกราบเรียนมาเพื่อโปรดทราบ/จึงเรียนยืนยันมา/จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ (อย่างย้ง)

ณัฐจักรี อนันตศิลป์

(นางณัฐจักรี อนันตศิลป์)

เลขาธิการคณะรัฐมนตรี

กองพัฒนาศาสตร์และติดตามนโยบายพิเศษ

โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๑๖๓๒ (วันจันทร์), ๑๕๓๒ (ปัญหารีย์)

โทรสาร ๐ ๒๒๘๐ ๑๔๔๖ www.soc.go.th

ไปรษณีย์อิเล็กทรอนิกส์ saraban@soc.go.th

หมายเหตุ	อัยการสูงสุด	: จึงกราบเรียนมาเพื่อโปรดทราบ
	รอง-นรม., รัฐ-นร., กระทรวง	: จึงเรียนยืนยันมา
	องค์กรอิสระ, กรม	: จึงเรียนมาเพื่อโปรดทราบ

บัญชีรายชื่อผู้ที่เกี่ยวข้องซึ่งได้แจ้งเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์
ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ให้ทราบ ดังนี้

๑. รองนายกรัฐมนตรี (นายภูมิธรรม เวชยชัย)
๒. รองนายกรัฐมนตรี (นายสุริยะ จึงรุ่งเรืองกิจ)
๓. รองนายกรัฐมนตรี (นายพีระพันธุ์ สาลีรัฐวิภาค)
๔. รองนายกรัฐมนตรี (นายพิชัย ชุณหวชิร)
๕. รองนายกรัฐมนตรี (นายประเสริฐ จันทรรวงทอง)
๖. รัฐมนตรีประจำสำนักนายกรัฐมนตรี (นายชูศักดิ์ ศิรินิล)
๗. รัฐมนตรีประจำสำนักนายกรัฐมนตรี (นางสาวจิราพร สินธุไพร)
๘. รัฐมนตรีประจำสำนักนายกรัฐมนตรี (นายสุชาติ ตันเจริญ)
๙. รัฐมนตรีว่าการกระทรวงกลาโหม
๑๐. รัฐมนตรีว่าการกระทรวงการคลัง
๑๑. รัฐมนตรีว่าการกระทรวงการต่างประเทศ
๑๒. รัฐมนตรีว่าการกระทรวงการท่องเที่ยวและกีฬา
๑๓. รัฐมนตรีว่าการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๑๔. รัฐมนตรีว่าการกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
๑๕. รัฐมนตรีว่าการกระทรวงเกษตรและสหกรณ์
๑๖. รัฐมนตรีว่าการกระทรวงคมนาคม
๑๗. รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
๑๘. รัฐมนตรีว่าการกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
๑๙. รัฐมนตรีว่าการกระทรวงพลังงาน
๒๐. รัฐมนตรีว่าการกระทรวงพาณิชย์
๒๑. รัฐมนตรีว่าการกระทรวงมหาดไทย
๒๒. รัฐมนตรีว่าการกระทรวงยุติธรรม
๒๓. รัฐมนตรีว่าการกระทรวงแรงงาน
๒๔. รัฐมนตรีว่าการกระทรวงวัฒนธรรม
๒๕. รัฐมนตรีว่าการกระทรวงศึกษาธิการ
๒๖. รัฐมนตรีว่าการกระทรวงสาธารณสุข
๒๗. รัฐมนตรีว่าการกระทรวงอุตสาหกรรม
๒๘. ปลัดสำนักนายกรัฐมนตรี
๒๙. เลขาธิการนายกรัฐมนตรี
๓๐. ผู้อำนวยการสำนักข่าวกรองแห่งชาติ
๓๑. ผู้อำนวยการสำนักงบประมาณ
๓๒. เลขาธิการสภาความมั่นคงแห่งชาติ

๓๓. เลขาธิการคณะกรรมการกฤษฎีกา
๓๔. เลขาธิการคณะกรรมการข้าราชการพลเรือน
๓๕. เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
๓๖. เลขาธิการคณะกรรมการพัฒนาระบบราชการ
๓๗. เลขาธิการคณะกรรมการส่งเสริมการลงทุน
๓๘. เลขาธิการสำนักงานทรัพยากรน้ำแห่งชาติ
๓๙. ผู้อำนวยการสำนักงานขับเคลื่อนการปฏิรูปประเทศ ยุทธศาสตร์ชาติ และการสร้างความสามัคคีปรองดอง
๔๐. ผู้อำนวยการสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ
๔๑. ผู้อำนวยการรักษาความมั่นคงภายในราชอาณาจักร
๔๒. ผู้อำนวยการศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล
๔๓. ผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติ
๔๔. เลขาธิการคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ
๔๕. เลขาธิการราชบัณฑิตยสภา
๔๖. ผู้บัญชาการตำรวจแห่งชาติ
๔๗. เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
๔๘. เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ
๔๙. เลขาธิการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้
๕๐. เลขาธิการคณะกรรมการนโยบายเขตพัฒนาพิเศษภาคตะวันออก
๕๑. อธิบดีกรมประชาสัมพันธ์
๕๒. ผู้อำนวยการสำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม
๕๓. เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
๕๔. เลขาธิการพระราชวัง
๕๕. เลขาธิการวุฒิสภา
๕๖. เลขาธิการสภาผู้แทนราษฎร
๕๗. เลขาธิการสำนักงานศาลรัฐธรรมนูญ
๕๘. เลขาธิการสำนักงานศาลยุติธรรม
๕๙. เลขาธิการสำนักงานศาลปกครอง
๖๐. เลขาธิการคณะกรรมการการเลือกตั้ง
๖๑. เลขาธิการสำนักงานผู้ตรวจการแผ่นดิน
๖๒. ผู้ว่าการตรวจเงินแผ่นดิน
๖๓. เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
๖๔. เลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ
๖๕. อัยการสูงสุด

บัญชีสำเนาหนังสือที่ส่งมาด้วย

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

๑. สำเนาหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ด่วนที่สุด ที่ สกมช ๐๘๑๐/๓๕๗๑ ลงวันที่ ๑๖ พฤษภาคม ๒๕๖๘
๒. สำเนาหนังสือกระทรวงกลาโหม ด่วนที่สุด ที่ กท ๐๒๐๗/๑๑๗๔ ลงวันที่ ๑๘ มิถุนายน ๒๕๖๘
๓. สำเนาหนังสือกระทรวงการคลัง ด่วนที่สุด ที่ กค ๐๒๐๒/๑๑๑๒๒ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๘
๔. สำเนาหนังสือกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ด่วนที่สุด ที่ พม ๐๒๐๙/๑๓๐๒๗
ลงวันที่ ๑๖ กรกฎาคม ๒๕๖๘
๕. สำเนาหนังสือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ด่วนที่สุด ที่ ดศ ๐๑๐๐.๔/๒๔๘
ลงวันที่ ๒๕ กรกฎาคม ๒๕๖๘
๖. สำเนาหนังสือกระทรวงแรงงาน ด่วนที่สุด ที่ รง ๐๒๐๑.๒/๒๓๒๙ ลงวันที่ ๑๗ กรกฎาคม ๒๕๖๘
๗. สำเนาหนังสือกระทรวงศึกษาธิการ ด่วนที่สุด ที่ ศธ ๐๒๐๒.๒/๑๙๙๙ ลงวันที่ ๑๗ มิถุนายน ๒๕๖๘
๘. สำเนาหนังสือกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/๒๓๔๐ ลงวันที่ ๒๓ มิถุนายน ๒๕๖๘
๙. สำเนาหนังสือสำนักเลขาธิการนายกรัฐมนตรี ที่ นร ๐๔๐๘/๗๔๕๗ ลงวันที่ ๙ กรกฎาคม ๒๕๖๘
๑๐. สำเนาหนังสือสำนักงานกบประมาณ ด่วนที่สุด ที่ นร ๐๗๐๘/๖๘๔ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๘
๑๑. สำเนาหนังสือสำนักงานคณะกรรมการกฤษฎีกา ด่วนที่สุด ที่ นร ๐๙๐๙/๘๘ ลงวันที่ ๓๐ พฤษภาคม ๒๕๖๘
๑๒. สำเนาหนังสือสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ ที่ นร ๑๑๑๖/๒๘๕๓
ลงวันที่ ๑๗ มิถุนายน ๒๕๖๘
๑๓. สำเนาหนังสือสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ด่วนที่สุด ที่ สพร ๒๕๖๘/๑๕๙๐
ลงวันที่ ๒๗ พฤษภาคม ๒๕๖๘

๑๖ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการ
ป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

สิ่งที่ส่งมาด้วย รายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ครั้งที่ ๓/๒๕๖๗

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอ เรื่อง
กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มาเพื่อคณะรัฐมนตรีพิจารณาเห็นชอบ โดยเรื่องนี้เข้าข่ายที่จะให้นำเสนอ
คณะรัฐมนตรีได้ตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘
มาตรา ๔ (๑)

ทั้งนี้ เรืองดังกล่าวมีรายละเอียด ดังนี้

๑. เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี

การเสนอกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับ
หน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มีความจำเป็นต้องเสนอคณะรัฐมนตรี
เพื่อพิจารณาและให้ความเห็นชอบ เนื่องจากการดำเนินการตาม พระราชบัญญัติการรักษาความมั่นคง
ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) ซึ่งกำหนดให้ คณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่เสนอแนะและให้ความเห็นต่อ คณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคง
ปลอดภัยไซเบอร์

นอกจากนี้ มาตรา ๒๒ (๕) และ (๖) ของพระราชบัญญัติฉบับเดียวกัน ได้กำหนดให้
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่ดำเนินการและประสานงาน
กับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงเฝ้าระวัง ติดตาม
วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ซึ่งเป็นหน้าที่สำคัญที่เกี่ยวข้องโดยตรงกับการดำเนินการตาม
กรอบแนวทางที่เสนอ

ดังนั้น เรื่องนี้จึงเข้าข่ายเรื่องที่ต้องเสนอคณะรัฐมนตรีตาม พระราชกฤษฎีกาว่าด้วยการ
เสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑) เรื่องที่กฎหมายกำหนดให้เป็นอำนาจ
หน้าที่ของคณะรัฐมนตรีหรือให้ต้องเสนอคณะรัฐมนตรี

๒. ความเร่งด่วนของเรื่อง

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีความจำเป็น
ที่จะต้องเสนอขอความเห็นชอบและอนุมัติในต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัย
ไซเบอร์ให้กับหน่วยงานของรัฐจากคณะรัฐมนตรี เนื่องจากปัจจุบันมีการรั่วไหลของข้อมูลส่วนบุคคล
เป็นจำนวนมาก จึงขอความกรุณาเสนอเรื่องนี้ต่อคณะรัฐมนตรีภายในเดือนมิถุนายน ๒๕๖๘

๓. สาระสำคัญและข้อเท็จจริง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ โดยมีวาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ จึงได้เสนอแนวทางขับเคลื่อนการแก้ไขปัญหาเชิงระบบสำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อเป็นกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ดังนี้

๑) การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทางมาตรฐาน ISO/IEC 27001 หรือ NIST Cyber Security Framework ในการออกแบบ พัฒนา และบำรุงรักษาระบบงัดใช้ข้อมูลจริงในขั้นตอนการพัฒนาระบบ หรือกำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน รวมทั้งกำหนดเกณฑ์สำหรับการเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการรับรองทางความปลอดภัย ตลอดจนกำหนดให้มีการกำกับดูแลและติดตาม รวมทั้งการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒) หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓) จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔) กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕) จัดให้มีกลไกการเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖) สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗) หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

๘) ให้หน่วยงานปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ซึ่งสอดคล้องกับนโยบาย Cloud First Policy เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัล

ทั้งนี้ ที่ประชุมมีมติ เห็นชอบ แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่ สกมช. เสนอ และมอบหมายให้ สกมช. เสนอแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ให้คณะรัฐมนตรีพิจารณาประกาศให้ทุกหน่วยงานถือปฏิบัติ ต่อไป

๔. ประโยชน์และผลกระทบ

การดำเนินการตามกรอบแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ จะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของรัฐบาลมีความมั่นคงปลอดภัยมากยิ่งขึ้น เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน อีกทั้งยังเป็นการสนับสนุนนโยบายดิจิทัลของประเทศไทย ทำให้ประเทศไทยมีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ทัดเทียมกับระดับสากล

ผลกระทบที่จะเกิดขึ้น มาตรการนี้จะเพิ่มภาระบางส่วนต่อประชาชนและหน่วยงานของรัฐ แต่จะช่วยลดความเสี่ยงด้านไซเบอร์ในระยะยาว ทำให้บริการของภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น

๕. ค่าใช้จ่ายและแหล่งที่มา หรือการสูญเสียรายได้

- ไม่มี

๖. ความเห็นหรือความเห็นชอบ/อนุมัติของหน่วยงานที่เกี่ยวข้อง

สกมช. ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ โดยมีวาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล และที่ประชุมมีมติ เห็นชอบ แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่ สกมช. เสนอ และมอบหมายให้ สกมช. เสนอแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ให้คณะรัฐมนตรีพิจารณาประกาศให้ทุกหน่วยงานถือปฏิบัติ ต่อไป

๗. ขอกฎหมายและมติคณะรัฐมนตรีที่เกี่ยวข้อง

- ไม่มี

๘. ข้อเสนอของหน่วยงานของรัฐ/คณะกรรมการเจ้าของเรื่อง

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้ว ขอเสนอคณะรัฐมนตรีเพื่อโปรดพิจารณาให้ความเห็นชอบ ดังต่อไปนี้

๘.๑ เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

๘.๒ อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์
ให้กับระบบงานของหน่วยงาน ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณานำเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ



(นายประเสริฐ จันทรวงทอง)

รองนายกรัฐมนตรี

ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕

ไปรษณีย์อิเล็กทรอนิกส์ : thaicert@ncsa.or.th

สำเนาถูกต้อง

ปัญญาชัย ศักดิ์ประเสริฐไชย

(นางสาวปัญญารีย์ ศิประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

รายงานการประชุม
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ครั้งที่ ๓/๒๕๖๗
วันพุธที่ ๓๐ ตุลาคม ๒๕๖๗ เวลา ๐๙.๐๐ น.
ณ ห้องประชุมคณะกรรมการ บมจ. โทรคมนาคมแห่งชาติ ชั้น ๑๐
อาคารสำนักงานใหญ่ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
และผ่านสื่ออิเล็กทรอนิกส์

รายชื่อคณะกรรมการผู้เข้าร่วมการประชุม

- | | |
|--|---------------------|
| ๑. นายประเสริฐ จันทรรวงทอง | ประธานกรรมการ |
| ๒. พลเรือเอก สุพัตต์ ยุทธวงศ์
รองปลัดกระทรวงกลาโหม
ผู้แทน รัฐมนตรีว่าการกระทรวงกลาโหม | กรรมการ |
| ๓. นายประเสริฐ จันทรรวงทอง
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | กรรมการ |
| ๔. นายเฉลิมศักดิ์ เลิศวงศ์เสถียร
ที่ปรึกษาด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ผู้แทน ปลัดกระทรวงการคลัง | กรรมการ |
| ๕. นายไตรยฤทธิ์ เตมียัง
รองปลัดกระทรวงยุติธรรม
ผู้แทน ปลัดกระทรวงยุติธรรม | กรรมการ |
| ๖. พลตำรวจตรี ชูศักดิ์ ขนาดนิค
ผู้บังคับการ กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี
ผู้แทน ผู้บัญชาการตำรวจแห่งชาติ | กรรมการ |
| ๗. นายรัชกรณ นภาพรพัฒน์
รองเลขาธิการสภาความมั่นคงแห่งชาติ
ผู้แทน เลขาธิการสภาความมั่นคงแห่งชาติ | กรรมการ |
| ๘. นายปริญญา หอมเอนก
ผู้ทรงคุณวุฒิ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ | กรรมการ |
| ๙. พันตำรวจเอก ญาณพล ยั่งยืน
ผู้ทรงคุณวุฒิ ด้านวิศวกรรมศาสตร์ | กรรมการ |
| ๑๐. นายไพบุลย์ อมรปัญญาเกียรติ
ผู้ทรงคุณวุฒิ ด้านกฎหมาย | กรรมการ |
| ๑๑. นายวิเชฐ ตันติวานิช
ผู้ทรงคุณวุฒิ ด้านการเงิน | กรรมการ |
| ๑๒. พลอากาศตรี อมร ชมเชย
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | กรรมการและเลขานุการ |

รายชื่อคณะกรรมการผู้เข้าร่วมการประชุม ผ่านสื่ออิเล็กทรอนิกส์

- | | |
|--|---------|
| ๑. พลเอก มโน นุชเกษม | กรรมการ |
| ผู้ทรงคุณวุฒิ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร | |
| ๒. นายบดีนทร์ ทรัพย์สมบูรณ์ | กรรมการ |
| ผู้ทรงคุณวุฒิ ด้านสาธารณสุข | |

รายชื่อคณะกรรมการติดตามภารกิจ

- | | |
|---|---------|
| ๑. รองศาสตราจารย์ ปณิธาน วัฒนายากร | กรรมการ |
| ผู้ทรงคุณวุฒิ ด้านความสัมพันธ์ระหว่างประเทศ | |

รายชื่อผู้เข้าร่วมการประชุม

คณะทำงานของรองนายกรัฐมนตรี (นายประเสริฐ จันทรรวงทอง)

- | | |
|-----------------------------|--|
| ๑. นายพรณธนู สรรณางาชัย | ที่ปรึกษารัฐมนตรีว่าการ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม |
| ๒. นายอัฐฐเสฏฐ จุลเสฏฐพานิช | เลขานุการรัฐมนตรีว่าการ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม |

ผู้ติดตามรองปลัดกระทรวงกลาโหม

- | | |
|----------------------------|--|
| ๓. พลโท นรเศรษฐ์ พงษ์เจริญ | เจ้ากรมเทคโนโลยีกระทรวงกลาโหม |
| ๔. นายสุชนา พงษ์มา | |
| ๕. พันเอก สันต์ นันทขว้าง | ผู้อำนวยการกองแผนไซเบอร์ ศูนย์ไซเบอร์ฯ |

ผู้ติดตามผู้บังคับการ กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี

- | | |
|-----------------------------------|------------------------|
| ๖. พันตำรวจตรี อนุสรณ์ พิมพ์สว่าง | ผู้ติดตามผู้บังคับการฯ |
|-----------------------------------|------------------------|

ผู้ติดตามรองปลัดกระทรวงยุติธรรม

- | | |
|--------------------------|---|
| ๗. นางสาวธนวรรณ ท้วมยิ้ม | ผู้อำนวยการศูนย์สำนักเทคโนโลยีสารสนเทศ
และการสื่อสาร |
| ๘. นายรัตนพล รัตนพิทักษ์ | นักวิชาการคอมพิวเตอร์ปฏิบัติ |

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- | | |
|------------------------------------|--|
| ๙. พลตรีธีรวุฒิ วิทยากรณ์ | รองเลขาธิการคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ |
| ๑๐. นางสาวสายชล แซ่ลี | ผู้อำนวยการสำนักประสานงาน |
| ๑๑. พลอากาศตรี วุฒิกัทร จันทรสาร | ผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษา
ความมั่นคงปลอดภัยไซเบอร์ |
| ๑๒. พลอากาศตรี เฉลิมชัย วงษ์เกตุ | ผู้อำนวยการศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ |
| ๑๓. พันตำรวจเอก ณัทฤกษ์ พรหมจันทร์ | ผู้อำนวยการ สำนักบริหารโครงสร้างพื้นฐาน
สำคัญทางสารสนเทศ |
| ๑๔. พันโท ญาณินทร์ สุรพันธ์ไพโรจน์ | ผู้อำนวยการฝ่ายขับเคลื่อนยุทธศาสตร์ประเทศ
สำนักนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ |
| ๑๕. นายดนัยวิทย์ ชาญสมร | หัวหน้างานความร่วมมือต่างประเทศ |

- ๑๖.นายอดิศร พิมลรัตน์
- ๑๗.นายอรรถพล อมาตยกุล
- ๑๘.นางสาวกนกวรรณ พรศุภปัทมา
- ๑๙.นางสาวจิรนนท์ รื่นสนธิ์
- ๒๐.นายณัช ธนภัทรภรณ์
- ๒๑.นางสาวสุติพร แสงแก้ว
- ๒๒.นางสาวลัดดา จิตแมน
- ๒๓.นายฐิติพงศ์ พ่วงเจริญ
- ๒๔.นายชนะพล วศินวิทย์
- ๒๕.นายธิตูฒิ อัมระนันท์
- ๒๖.นางสาวนวลนภา คู่กระโทก
- ๒๗.นางสาวณิชาภัทร ศรีรัตน์

สำนักประสานงาน
เจ้าหน้าที่วิชาชีพเฉพาะ ด้านกฎหมาย
เจ้าหน้าที่วิชาชีพเฉพาะ ด้านเทคโนโลยีสารสนเทศ
เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะ ด้านไซเบอร์
เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะ ด้านไซเบอร์
เจ้าหน้าที่กลุ่มวิชาชีพเฉพาะ ด้านไซเบอร์
เจ้าหน้าที่กลุ่มปฏิบัติงานทั่วไป ด้านการจัดการ
เจ้าหน้าที่กลุ่มปฏิบัติงานทั่วไป ด้านการจัดการ
เจ้าหน้าที่กลุ่มปฏิบัติงานทั่วไป ด้านการจัดการ
สนับสนุนงานเทคโนโลยีสารสนเทศ
สนับสนุนงานเทคโนโลยีสารสนเทศ
เจ้าหน้าที่ประสานงานโครงการ
เจ้าหน้าที่ประสานงานโครงการ

รายชื่อผู้เข้าร่วมการประชุม ผ่านสื่ออิเล็กทรอนิกส์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- | | |
|---------------------------------|--|
| ๒๘.พลอากาศตรี จเด็จ คุณะก้องกิจ | ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ |
| ๒๙.นาวาเอก ศิริเนตร รักษ์วงศ์ | ผู้ทรงคุณวุฒิพิเศษ ๑ |
| ๓๐.นางพัชัญชิตา ไกรแสงศรี | ผู้เชี่ยวชาญพิเศษสำนักบริหารกลาง ๑ |
| ๓๑.พันตรี ปวิข บูรพาชลทิศน์ | รักษาการ ผู้อำนวยการสำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ |
| ๓๒.นายภาณุพล เหนียวแน่น | เจ้าหน้าที่วิชาชีพเฉพาะ ด้านเทคโนโลยีสารสนเทศ |
| ๓๓.นายจิรศักดิ์ วิชัยกุล | |
| ๓๔.นายทงศักดิ์ พุกคล้าย | |

เอกสารประกอบการประชุม

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๒. รายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗
๓. แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของ สหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ ๓ ปี (พ.ศ. ๒๕๖๘-๒๕๗๐)
๔. ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗
๕. ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

๖. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ลงวันที่ ๒๑ กุมภาพันธ์ ๒๕๖๓
๗. คำสั่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ ๒/๒๕๖๗ ลงวันที่ ๓ กันยายน ๒๕๖๗ เรื่อง แต่งตั้งคณะกรรมการสรรหากรรมการผู้ทรงคุณวุฒิ ใน กบส.
๘. หนังสือ สกมช. ด่วนที่สุด ที่ ๐๙๐๐/๕๑๘๔ เรื่อง (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.
๙. คำสั่งแต่งตั้งคณะทำงานดำเนินการเตรียมความพร้อมระบบสารสนเทศเพื่อเข้าสู่ยุคควอนตัม
๑๐. หนังสือสำนักงาน ก.พ.ร. ที่ นร ๑๒๐๖/๕๐๕๓ ลงวันที่ ๗ ธันวาคม ๒๕๖๖ เรื่อง การชี้แจงแนวทางการสมัครและหลักเกณฑ์การพิจารณารางวัลเลิศรัฐ ประจำปี ๒๕๖๗
๑๑. ประกาศคณะกรรมการพัฒนาระบบราชการ เรื่อง ผลการพิจารณารางวัลเลิศรัฐ ประจำปี ๒๕๖๗ ประกาศ ณ วันที่ ๓ กันยายน ๒๕๖๗
๑๒. หนังสือสำนักงาน ก.พ.ร. ที่ นร ๑๒๐๖/๒๖๒๑ ลงวันที่ ๖ กันยายน ๒๕๖๗ เรื่อง ขอเชิญร่วมงานเสวนาวิชาการและพิธีมอบรางวัลเลิศรัฐ ประจำปี ๒๕๖๗
๑๓. รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ประจำปี ๒๕๖๗ (ห้วง ๑ ตุลาคม ๒๕๖๖ - ๓๐ กันยายน ๒๕๖๗)
๑๔. (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือทางวิชาการระหว่างสถาบันบัณฑิตพัฒนบริหารศาสตร์ โดยคณะนิติศาสตร์กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๕. (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมทักษะและการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ มหาวิทยาลัยสวนดุสิต
๑๖. (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ กับ กรมส่งเสริมการเรียนรู้
๑๗. หนังสือ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ด่วนที่สุด ที่ สกมช ๐๘๑๐/๖๐๒๑ ลงวันที่ ๑๗ ตุลาคม ๒๕๖๗ เรื่อง การจัดทำ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
๑๘. (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
๑๙. หนังสือ กระทรวงยุติธรรม ด่วนที่สุด ที่ ยธ ๐๒๐๐๖/๑๒๓๔๓ ลงวันที่ ๑๖ ตุลาคม ๒๕๖๗ เรื่อง ขอจัดส่ง (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
๒๐. (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ กระทรวงยุติธรรม

เริ่มประชุม ๐๙.๓๐ น.

ระเบียบวาระที่ ๑ เรื่องที่ประธานแจ้งให้ที่ประชุมทราบ

ขอขอบคุณคณะกรรมการทุกท่านที่เสียสละเวลามาร่วมการประชุมในครั้งนี้ กระผมมีเรื่องแรกที่ขอแสดงความยินดีที่หน่วยงานที่เรียกว่า Global Cybersecurity Index หรือ GCI ซึ่งได้ประเมินความมั่นคงปลอดภัยทางไซเบอร์ ได้ประเมินประเทศไทยซึ่งเดิมอยู่อันดับที่ ๔๔ ได้รับการประเมินขึ้นเป็นอันดับที่ ๗ ถือว่าขึ้นมาได้หลายอันดับมาก โดยปกติจะขึ้นเป็นตามลำดับขั้น แต่สามารถขึ้นมาเป็นได้ถึงลำดับที่ ๗ ถือว่าประสบความสำเร็จในด้านนี้พอสมควร เพราะฉะนั้นขอให้ ดำเนินการต่อเพราะเรื่อง Cybersecurity สามารถส่งผลกระทบต่อการลงทุน และภาพลักษณ์ของประเทศ เพราะถ้าสิ่งเหล่านี้มีความมั่นคงจะทำให้ นักลงทุนสนใจที่จะมาลงทุนในประเทศไทย ทำให้มีความมั่นใจมากขึ้น ที่ผ่านมาในปี พ.ศ. ๒๕๖๗ ได้มีบริษัทใหญ่เข้ามาลงทุนแล้ว อาทิ Google ในปี ๒๕๖๘ คาดว่าจะมีบริษัทใหญ่ ๆ อีก ๒ บริษัท ที่จะมาลงทุนด้านไซเบอร์ ด้านเทคโนโลยีดิจิทัล ในประเทศไทย ซึ่งจะทำให้ในรอบ ๑ปี อาจจะมีการลงทุนกว่าแสนล้านบาท ซึ่งจะเป็นอุตสาหกรรมลงทุนที่มีมูลค่าสูงที่สุดในบรรดาอุตสาหกรรมทุกอย่างประเภท เช่นอุตสาหกรรมเทคโนโลยีสารสนเทศ เป็นตัวเลือกที่ส่งเสริมมากกว่าภาคอื่น ๆ ทั้งนี้ ขอขอบคุณคณะกรรมการทุกท่านที่ได้มีส่วนช่วยแล้วก็ได้นำให้ข้อคิดต่าง ๆ สำหรับการประชุมในวันนี้มีวาระหลายเรื่องด้วยกัน เป็นเรื่องเพื่อทราบทั้งหมด ๙ เรื่องเรื่องเพื่อพิจารณา ๔ เรื่อง ก็ขอให้ฝ่ายเลขาฯ ได้ดำเนินการตามนโยบายประชุมต่อไป

ระเบียบวาระที่ ๒ เรื่องที่ประธานแจ้งให้ที่ประชุมทราบ

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ได้รายงานให้ที่ประชุมทราบว่าสืบเนื่องจากการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ ฝ่ายเลขานุการฯ ได้จัดทำ (ร่าง) รายงานการกประชุมและได้แจ้งเวียนให้คณะกรรมการทุกท่านแล้ว ซึ่งคณะกรรมการฯ ได้พิจารณาแล้วไม่มีข้อแก้ไข โดยในรายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๐ กรกฎาคม ๒๕๖๗ มีประเด็นเพื่อพิจารณา จำนวน ๘ เรื่อง ดังนี้

๒.๑ พิจารณานวทางการยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตามดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ของโลก (Global Cybersecurity Index) ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU)

๒.๒ (ร่าง) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ.

๒.๓ พิจารณาให้ความเห็นชอบเสนอ (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ต่อคณะรัฐมนตรี

๒.๔ แต่งตั้งคณะกรรมการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๕ บันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- ๒.๕.๑ (ร่าง) บันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ กระทรวงคมนาคม
- ๒.๕.๒ (ร่าง) บันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ กระทรวงพลังงาน
- ๒.๕.๓ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการวิจัยและพัฒนา ด้านความมั่นคงปลอดภัยไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สำนักงานนวัตกรรมแห่งชาติ
- ๒.๕.๔ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมการพัฒนาทักษะการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ มหาวิทยาลัยราชภัฏร้อยเอ็ด มหาวิทยาลัยกรุงเทพ และมหาวิทยาลัยหอการค้าไทย
- ๒.๕.๕ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมการพัฒนาทักษะการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ มหาวิทยาลัยสงขลานครินทร์
- ๒.๕.๖ (ร่าง) บันทึกข้อตกลงความร่วมมือด้านการวิจัยและพัฒนา ด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลระหว่าง สำนักงานการวิจัยแห่งชาติกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ๒.๕.๗ (ร่าง) บันทึกข้อตกลงความร่วมมือในการจัดทำพร้อมทั้งเผยแพร่สื่อประชาสัมพันธ์ ภายใต้โครงการ “Digital Vaccine” ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ ๑๒ หน่วยงาน
- ๒.๖ (ร่าง) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้ และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.
- ๒.๗ พิจารณาแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ใน คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
- ๒.๘ ขออนุมัติหลักการการไปปฏิบัติงาน การอบรม ประชุม สัมมนา ของเลขาธิการ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- คณะกรรมการฯ พิจารณารับรองรายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ โดยไม่มีการแก้ไข

มติที่ประชุม รับรองรายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ โดยไม่มีการแก้ไข

ระเบียบวาระที่ ๓ เรื่องเพื่อทราบ

๓.๑ พิจารณาทบทวนแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ ๓ ปี (พ.ศ. ๒๕๖๘ - ๒๕๗๐)

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมขอให้ พันโท ญาณินทร์ สุรพันธ์ไพโรจน์ ผู้อำนวยการฝ่ายขับเคลื่อนยุทธศาสตร์ประเทศ สำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ความเป็นมา

ดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ของโลก (Global Cybersecurity Index : GCI) จัดทำโดยสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ซึ่งเป็นตัวชี้วัดในการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ ๕ ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity Development) และด้านความร่วมมือ (Cooperation) โดยผลการจัดอันดับ GCI ประจำปี พ.ศ. ๒๕๖๓ (GCI๒๐๒๐) ซึ่งเป็นการจัดอันดับจากการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ในหมู่ประเทศสมาชิก ITU ปรากฏว่า ประเทศไทยได้รับการจัดอันดับที่ ๔๔ จากทั้งหมด ๑๙๔ ประเทศ และอยู่ในอันดับ ๕ ของประเทศสมาชิกอาเซียน

สภมช. จึงได้ปรับปรุง เพิ่มเติม แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ ๓ ปี เป็นที่เรียบร้อยแล้ว และได้นำเรียนในที่ประชุม สภมช. ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ ณ ห้องประชุมวิภาวดี ชั้น ๓ อาคารสำนักงานปลัดกระทรวงพาณิชย์ โดยมี นายภูมิธรรม เวชยชัย รองนายกรัฐมนตรี เป็นประธานฯ มติที่ประชุม เห็นชอบร่างแนวทางดังกล่าว เป็นที่เรียบร้อยแล้ว

แต่เนื่องด้วยมีการปรับเปลี่ยนนายกรัฐมนตรีเป็น นางสาวแพทองธาร ชินวัตร จึงได้มีการทบทวนความเชื่อมโยงของแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าวให้มีความสอดคล้องของต่อคำแถลงนโยบายของคณะรัฐมนตรีปัจจุบัน ให้มีความทันสมัยมากยิ่งขึ้น

ประกอบกับ รายงานผลการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของ ITU ครั้งที่ ๕ ประจำปี พ.ศ. ๒๕๖๗ (GCI ๒๐๒๔) ประเทศไทยได้คะแนน ๙๙.๒๒/๑๐๐ และถูกจัดอยู่ในกลุ่ม Tier ๑: Role Modelling โดยคะแนนดังกล่าว ทำให้ประเทศไทยจัดเป็นลำดับ ๗ จากการประเมิน ๑๙๔ ประเทศทั่วโลก และ ลำดับที่ ๔ ในกลุ่มประเทศสมาชิกอาเซียน

ข้อรายงาน

สภามช. จึงได้ปรับปรุงความเชื่อมั่นของแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าว **ให้สอดคล้องต่อ นโยบายของคณะรัฐมนตรี ประเด็นนโยบายเร่งด่วน นโยบายที่ ๙ รัฐบาลจะเร่งแก้ปัญหาอาชญากรรม อาชญากรรมออนไลน์ และได้อัปเดตข้อมูลผลการประเมินครั้งล่าสุดให้ทันสมัย สอดคล้องต่อสถานการณ์ในปัจจุบัน**

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบ ดังนี้

(๑) รับทราบการปรับแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ ๓ ปี (พ.ศ. ๒๕๖๘-๒๕๗๐) สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

(๒) มอบหมายให้ฝ่ายเลขานุการนำแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าว ไปขับเคลื่อนและบูรณาการในการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง และให้นำไปปรับปรุงในขั้นตอนการจัดทำนโยบายและแผนฉบับต่อไป

นายวิเชฐ ตันติวานิช กรรมการผู้ทรงคุณวุฒิด้านการเงิน ขอให้ฝ่ายเลขานุการชี้แจงรายละเอียดเพิ่มเติม เพราะมีการยกระดับดีขึ้นมาก

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ขออนุญาตชี้แจงให้ที่ประชุมทราบเกี่ยวกับการประเมินในส่วนของมาตรการทางกฎหมายสิ่งที่เปลี่ยนแปลงและทำให้ยกระดับขึ้นมาได้ เพราะเมื่อการวัดครั้งที่ผ่านมา ประเทศไทยมีการออก พ.ร.บ. ไซเบอร์ และ พ.ร.บ. PDPA ทำให้มีองค์กรมารับการขับเคลื่อนจึงเป็นหนึ่งในตัวแปรสำคัญที่จากเดิมจากตัวชี้วัดครั้งที่แล้วที่ยังไม่มีในส่วนของกฎหมายช่วยในการขับเคลื่อนครั้งนี้ และอีกส่วนหนึ่งในมาตรการทางด้านเทคนิค นอกเหนือจากการตั้ง ThaiCERT แล้ว ยังสนับสนุน ส่งเสริมให้เกิด SectoralCERT เพื่อให้ครอบคลุม ๗ Sector ในส่วนขององค์กรที่ได้เริ่มพัฒนามาทั้งในส่วนของ สภามช. และ สคส. รวมทั้งองค์กรอื่น ๆ ที่ดำเนินการร่วมกัน ซึ่งในส่วนนี้มีความก้าวหน้า แต่ยังต้องมีการปรับปรุงในเรื่องของความเข้มแข็งในองค์กรที่จะขับเคลื่อนในเรื่องนี้ต่อไป ส่วนเรื่อง Capaticy Development การพัฒนาบุคลากรได้มีการดำเนินการโครงการเร่งรัดพัฒนาบุคลากรทางด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีการดำเนินการในห้วงของการประเมินในครั้งนี้ที่ผ่านมา จึงมีความก้าวหน้าจากเป้าหมาย ๑,๐๐๐ คน สามารถพัฒนาได้ ๔,๕๐๐ คน ซึ่งเป็นหนึ่งในตัวแปรที่สำคัญที่ได้ยกระดับในเรื่องนี้ และที่สำคัญอีกส่วนหนึ่งคือความร่วมมือของภาครัฐ ภาคเอกชน ทั้งภายในและภายนอกประเทศ ที่ได้มีความร่วมมือทางด้านไซเบอร์หลังจากที่มีหน่วยงานรับผิดชอบโดยตรง และมีการขับเคลื่อนอย่างต่อเนื่อง อีกทั้งเป็นปัจจัยเสริม ทำให้คะแนนดีขึ้นจากเดิม ๙๐ เป็น ๙๙ ส่งผลให้ได้ลำดับที่ดีขึ้น

มติที่ประชุม รับทราบการปรับแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ ๓ ปี (พ.ศ. ๒๕๖๘-๒๕๗๐) สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง และมอบหมาย

ให้ฝ่ายเลขานุการนำแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ดังกล่าวไปขับเคลื่อนและบูรณาการในการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง และให้นำไปปรับปรุงในขั้นตอนการจัดทำนโยบายและแผนฉบับต่อไป

๓.๒ รายงานผลการจัดทำประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๒ ฉบับ

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมนางสาวตรุณี พิกุลทอง ผู้อำนวยการสำนักกฎหมาย เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ข้อกฎหมาย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙ บัญญัติว่า “คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๔) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

(๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์”

ขอรายงาน

๑. ในคราวการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ ที่ประชุมได้พิจารณาและมีมติเห็นชอบ (ร่าง) ประกาศ กมช. จำนวน ๒ ฉบับ ดังนี้

๑.๑ (ร่าง) ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ.

๑.๒ (ร่าง) ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ.

ทั้งนี้ ที่ประชุมได้มอบหมายให้ฝ่ายเลขานุการนำ (ร่าง) ประกาศ กมช. จำนวน ๒ ฉบับ ดังกล่าว เสนอผู้มีอำนาจเพื่อพิจารณาลงนาม ก่อนนำไปประกาศในราชกิจจานุเบกษาเพื่อใช้บังคับต่อไป

๒. สกมช. ได้ดำเนินการเสนอ (ร่าง) ประกาศ กมช. ทั้งสองฉบับดังกล่าวข้างต้น ต่อ รองนายกรัฐมนตรี (นายภูมิธรรม เวชยชัย) ปฏิบัติหน้าที่ ประธาน กมช. เพื่อพิจารณาลงนามเรียบร้อยแล้ว

ซึ่งเมื่อวันที่ ๓ กันยายน ๒๕๖๗ ประธาน กมช. ได้ลงนามใน (ร่าง) ประกาศ กมช. ทั้งสองฉบับดังกล่าวเรียบร้อยแล้ว พร้อมนี้ สกช. ได้จัดส่งประกาศ กมช. ทั้งสองฉบับดังกล่าวไปประกาศในราชกิจจานุเบกษา เรียบร้อยด้วยแล้ว

๓. เมื่อวันที่ ๑๐ กันยายน ๒๕๖๗ สำนักเลขาธิการคณะรัฐมนตรี ได้นำประกาศ กมช. จำนวน ๒ ฉบับ ดังกล่าว ประกาศลงในราชกิจจานุเบกษาเรียบร้อยแล้ว โดยมีรายละเอียดดังนี้

๓.๑ ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้ และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗ ลงประกาศในราชกิจจานุเบกษา เล่มที่ ๑๔๑ ตอนพิเศษ ๒๔๘ ง ลงวันที่ ๑๐ กันยายน ๒๕๖๗ มีผลใช้บังคับเมื่อพ้นกำหนดหนึ่งปี นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป (ตั้งแต่วันที่ ๑๐ กันยายน ๒๕๖๘ เป็นต้นไป)

๓.๒ ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ระบบคลาวด์ พ.ศ. ๒๕๖๗ ลงประกาศในราชกิจจานุเบกษา เล่มที่ ๑๔๑ ตอนพิเศษ ๒๔๘ ง ลงวันที่ ๑๐ กันยายน ๒๕๖๗ มีผลใช้บังคับเมื่อพ้นกำหนดสองปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป (ตั้งแต่วันที่ ๑๐ กันยายน ๒๕๖๙ เป็นต้นไป)

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบผลการจัดทำประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๒ ฉบับ

มติที่ประชุม รับทราบผลการจัดทำประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๒ ฉบับ

๓.๓ รายงานความคืบหน้าการจัดทำ (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. และความคืบหน้าการสรรหาและแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมนางสาวดรุณี พิฤททอง ผู้อำนวยการสำนักกฎหมาย เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ข้อกฎหมาย

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๕ บัญญัติว่า “ให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” ประกอบด้วย

(๑) นายกรัฐมนตรี เป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ และเลขาธิการสภาความมั่นคงแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจาก ผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมาย ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงาน เป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อเสนอคณะรัฐมนตรีแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๗ วรคสอง ให้เป็นไปตามระเบียบที่คณะรัฐมนตรีกำหนดโดยการเสนอแนะของคณะกรรมการ”

มาตรา ๗ บัญญัติว่า “กรรมการผู้ทรงคุณวุฒิในคณะกรรมการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ ให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งกรรมการผู้ทรงคุณวุฒิแทนก็ได้

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมีได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่”

มาตรา ๑๒ บัญญัติว่า “ในการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการตามมาตรา ๙ ให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” ประกอบด้วย

(๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ได้แก่ ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคม ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงสาธารณสุข ผู้บัญชาการตำรวจแห่งชาติ ผู้บัญชาการทหารสูงสุด เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และเลขาธิการคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่งคณะกรรมการแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงาน เป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลที่เห็นสมควรเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด”

มาตรา ๑๕ บัญญัติว่า “ให้นำความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิใน กกม. โดยอนุโลม”

มาตรา ๒๕ วรรคหนึ่ง บัญญัติว่า “ให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินหกคน เป็นกรรมการ”

มาตรา ๒๕ วรรคสาม บัญญัติว่า “กรรมการผู้ทรงคุณวุฒิตามวรรคหนึ่ง ให้รัฐมนตรีแต่งตั้งจากบุคคลซึ่งมีความรู้ ความเชี่ยวชาญ และความสามารถเป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมายด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการดำเนินงานของ กบส. ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด”

๒. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ลงวันที่ ๒๑ กุมภาพันธ์ ๒๕๖๓

ข้อ ๓ กำหนดว่า “ให้คณะกรรมการสรรหา มีอำนาจหน้าที่ในการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

(๑) ให้คณะกรรมการสรรหา กำหนดความรู้ ความเชี่ยวชาญ ด้านที่ ประสงค์ จะให้มีการผู้ทรงคุณวุฒิ เช่น ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศ และการสื่อสารด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการดำเนินงานของคณะกรรมการเฉพาะด้านนั้น ๆ ไม่เกิน ๖ ด้าน พร้อมทั้งจำนวนกรรมการ แต่ละด้านที่จะเสนอให้มีการแต่งตั้ง

(๒) ให้กรรมการสรรหา ดำเนินการสรรหา เพื่อให้ได้มาซึ่งบุคคลที่มีความรู้ ความเชี่ยวชาญ และความสามารถเป็นที่ประจักษ์ในด้านที่กำหนดใน (๑) โดยมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามมาตรา ๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พร้อมทั้งประวัติย่อและคำยินยอมของผู้ที่ได้รับการเสนอชื่อ

(๓) ห้ามมิให้เสนอรายชื่อกรรมการสรรหาเป็นกรรมการผู้ทรงคุณวุฒิ

(๔) ก่อนการพิจารณาคัดเลือกให้เลขานุการรวบรวมรายชื่อตรวจสอบคุณสมบัติ ลักษณะต้องห้าม พร้อมทั้งประวัติและผลงานของผู้ที่ได้รับการเสนอชื่อและเสนอให้คณะกรรมการสรรหาพิจารณา

(๕) ให้คณะกรรมการสรรหา ดำเนินการคัดเลือกผู้ที่ได้รับการสรรหาเป็นกรรมการผู้ทรงคุณวุฒิที่จะมีในแต่ละด้านตาม (๑) ให้เหลือจำนวนด้านละหนึ่งคน และสรุปผลการคัดเลือกพร้อมทั้งประวัติ และผลงานของผู้ที่ได้รับการสรรหาเสนอต่อรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาส่งเสนอต่อรัฐมนตรีเพื่อมีคำสั่งแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิ

(๖) ให้คณะกรรมการสรรหา มีอำนาจดำเนินการอื่นใดเฉพาะในส่วนที่เกี่ยวข้องกับการสรรหา ได้เท่าที่จำเป็นและไม่ขัดหรือแย้งกับหลักเกณฑ์และวิธีการตามประกาศนี้

ในกรณีที่รัฐมนตรีไม่ให้ความเห็นชอบกับรายชื่อผู้ทรงคุณวุฒิที่เสนอรายใด ก็ให้มีการดำเนินการสรรหาบุคคลใหม่ โดยให้คณะกรรมการสรรหาชุดเดิมเป็นผู้มีหน้าที่และอำนาจ ในการดำเนินการจนกว่าจะได้กรรมการผู้ทรงคุณวุฒิครบตามจำนวนที่กฎหมายกำหนดโดยเร็ว”

ข้อรายงาน

๑. ความคืบหน้าการจัดทำ (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการ ผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.

๑.๑ ในคราวการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ (กมช.) ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ ที่ประชุมได้พิจารณา (ร่าง) ระเบียบ ว่าด้วย หลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ พ.ศ. และได้มีมติเห็นชอบ (ร่าง) ระเบียบดังกล่าว พร้อมทั้งมอบหมายให้ สกมช. นำ (ร่าง) ระเบียบดังกล่าวเสนอคณะรัฐมนตรี เพื่อพิจารณาต่อไป

๑.๒ เมื่อวันที่ ๒๕ กันยายน ๒๕๖๗ รองนายกรัฐมนตรี (นายประเสริฐ จันทรรวงทอง) ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ลงนามในหนังสือ ด่วนที่สุด ที่ สกมช ๐๙๐๐/๕๑๘๔ เรียง เลขานุการคณะรัฐมนตรี เพื่อพิจารณานำ (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์ และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. เสนอต่อคณะรัฐมนตรีเพื่อพิจารณามีมติให้ความเห็นชอบ

๑.๓ สถานะการดำเนินการจัดทำ (ร่าง) ระเบียบดังกล่าว ณ ปัจจุบันอยู่ระหว่างขั้นตอน กระบวนการของสำนักเลขาธิการคณะรัฐมนตรี ในการนำ (ร่าง) ระเบียบดังกล่าวเสนอต่อคณะรัฐมนตรี เพื่อพิจารณาต่อไป

๒. ความคืบหน้าการสรรหาและแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๒.๑ ในคราวการประชุม กมช. ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ ที่ประชุมได้มีการพิจารณาคัดเลือกรายชื่อผู้ได้รับการสรรหาและมีมติแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ขึ้นใหม่ (กกม.) แทนกรรมการผู้ทรงคุณวุฒิ ซึ่งพ้นจากตำแหน่งตามวาระ จำนวน ๔ คน ดังนี้

- | | |
|---------------------------------------|--|
| (๑) พลตำรวจตรี มนเทียร พันธ้อม | เป็นกรรมการผู้ทรงคุณวุฒิ
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ |
| (๒) รองศาสตราจารย์ อติวงศ์ สุชาโต | เป็นกรรมการผู้ทรงคุณวุฒิ
ด้านวิศวกรรมศาสตร์ |
| (๓) รองศาสตราจารย์ ยศชนัน วงศ์สวัสดิ์ | เป็นกรรมการผู้ทรงคุณวุฒิ
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร |
| (๔) นายปกาศิต เหลืองทอง | เป็นกรรมการผู้ทรงคุณวุฒิ
ด้านกฎหมาย |

ทั้งนี้ ที่ประชุมได้มอบหมายให้ฝ่ายเลขานุการการจัดทำ (ร่าง) ประกาศแต่งตั้ง กรรมการผู้ทรงคุณวุฒิใน กกม. เสนอต่อประธาน กมช. เพื่อพิจารณาลงนาม

๒.๒ สกมช. ได้จัดทำ (ร่าง) ประกาศ กมช. เรื่อง แต่งตั้งกรรมการผู้ทรงคุณวุฒิ ใน กกม. เสนอต่อ รองนายกรัฐมนตรี (นายภูมิธรรม เวชยชัย) ปฏิบัติหน้าที่ ประธาน กกม. เพื่อพิจารณาลงนาม แต่งตั้งบุคคลที่ได้รับการคัดเลือกจาก กกม. ตามข้อ ๒.๑ เป็นกรรมการผู้ทรงคุณวุฒิ ใน กกม. เรียบร้อยแล้ว ซึ่งเมื่อวันที่ ๓ กันยายน ๒๕๖๗ ประธาน กกม. ได้ลงนามในประกาศแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ใน กกม. ขึ้นใหม่ แทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระ เรียบร้อยแล้ว โดยประกาศดังกล่าวมีผลตั้งแต่วันที่ ๓ กันยายน ๒๕๖๗ เป็นต้นไป

๒.๓ เมื่อวันที่ ๑๒ กันยายน ๒๕๖๗ สกมช. ได้มีหนังสือ ที่ ๐๙๐๐/ว๔๖๗ แจ้งเวียนประกาศ กกม. เรื่อง แต่งตั้งกรรมการผู้ทรงคุณวุฒิ ใน กกม. ให้แก่บุคคลที่ได้รับการแต่งตั้ง เป็นกรรมการผู้ทรงคุณวุฒิ เพื่อโปรดทราบอำนาจหน้าที่และผลการแต่งตั้งดังกล่าวเรียบร้อยแล้ว

๓. ความคืบหน้าการสรรหาและแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหาร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑ ในคราวการประชุม กกม. ครั้งที่ ๒/๒๕๖๗ เมื่อวันที่ ๓๑ กรกฎาคม ๒๕๖๗ ที่ประชุมได้มีการพิจารณาและมีมติแต่งตั้งคณะกรรมการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหาร สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) และมอบหมายให้ฝ่ายเลขานุการฯ นำ (ร่าง) คำสั่งแต่งตั้งคณะกรรมการสรรหากรรมการผู้ทรงคุณวุฒิ ใน กบส. เสนอประธาน กกม. เพื่อลงนาม ก่อนดำเนินการในส่วนที่เกี่ยวข้อง ต่อไป

๓.๒ เมื่อวันที่ ๓ กันยายน ๒๕๖๗ รองนายกรัฐมนตรี (นายภูมิธรรม เวชยชัย) ปฏิบัติหน้าที่ ประธาน กกม. ได้ลงนามในคำสั่งแต่งตั้งคณะกรรมการสรรหากรรมการผู้ทรงคุณวุฒิ ใน กบส. เรียบร้อยแล้ว โดยมีองค์ประกอบ ดังนี้

(๑) นายภูษพงศ์ โนนไธสง	ประธานกรรมการสรรหา
(๒) พันเอก สรรพชัย หุวะนันทน์	กรรมการสรรหา
(๓) รองศาสตราจารย์ ชีรณี อจลากุล	กรรมการสรรหา
(๔) นายสุวิทย์ วิจิตรโสภาก	กรรมการสรรหา
(๕) ผู้ช่วยศาสตราจารย์ พงษ์ธนา วนิชย์กอบจินดา	กรรมการสรรหา
(๖) เลขธิการคณะกรรมการการักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ	เลขานุการ

๓.๓ ในการดำเนินการสรรหากรรมการผู้ทรงคุณวุฒิ ใน กบส. คณะกรรมการสรรหาฯ จำต้องดำเนินการตามหลักเกณฑ์ และวิธีการที่กำหนดไว้ในประกาศ กกม. ว่าด้วยหลักเกณฑ์และวิธีการสรรหา กรรมการผู้ทรงคุณวุฒิ ใน กบส. ลงวันที่ ๒๑ กุมภาพันธ์ ๒๕๖๓ โดยมีขั้นตอนกระบวนการดังนี้

ขั้นตอนที่ ๑ คณะกรรมการสรรหาฯ กำหนดความรู้ความเชี่ยวชาญด้านที่ประสงค์ จะให้มีกรรมการผู้ทรงคุณวุฒิ ไม่เกิน ๖ ด้าน พร้อมทั้งจำนวนกรรมการแต่ละด้านที่จะเสนอให้มีการแต่งตั้ง รวมทั้งกำหนดกรอบระยะเวลาและวิธีการในการดำเนินการสรรหา

ขั้นตอนที่ ๒ คณะกรรมการสรรหาฯ ดำเนินการสรรหาเพื่อให้ได้มาซึ่งบุคคลที่มี ความรู้ความเชี่ยวชาญและความสามารถเป็นที่ประจักษ์ในด้านที่กำหนดในขั้นตอนที่ ๑

ขั้นตอนที่ ๓ ฝ่ายเลขานุการดำเนินการรวบรวมรายชื่อตรวจสอบคุณสมบัติ ลักษณะต้องห้าม พร้อมทั้งประวัติและผลงานของผู้ได้รับการเสนอชื่อและเสนอให้คณะกรรมการสรรหา พิจารณา

ขั้นตอนที่ ๔ คณะกรรมการสรรหา ดำเนินการคัดเลือกผู้ที่ได้รับการสรรหา เป็นกรรมการผู้ทรงคุณวุฒิที่จะมีในแต่ละด้านตามขั้นตอนที่ ๑ ให้เหลือจำนวนด้านละหนึ่งคน และสรุปผลการคัดเลือกพร้อมทั้งประวัติและผลงานของผู้ที่ได้รับการสรรหา

ขั้นตอนที่ ๕ คณะกรรมการสรรหา นำสรุปผลการคัดเลือกพร้อมทั้งประวัติ และผลงานของผู้ที่ได้รับการสรรหาเสนอต่อรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณา นำเสนอต่อนายกรัฐมนตรีเพื่อมีคำสั่งแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิ

ขั้นตอนที่ ๖ นายกรัฐมนตรีลงนามในคำสั่งแต่งตั้งผู้ที่ได้รับการสรรหา เป็นกรรมการผู้ทรงคุณวุฒิ ใน กบส. (ชุดใหม่)

๓.๔ ปัจจุบันคณะกรรมการสรรหา ได้กำหนดให้มีการประชุม ครั้งที่ ๑/๒๕๖๗ ภายในเดือนพฤศจิกายน เพื่อพิจารณาดำเนินการกำหนดความรู้ความเชี่ยวชาญด้านที่ประสงค์จะให้ กรรมการผู้ทรงคุณวุฒิ ไม่เกิน ๖ ด้าน พร้อมทั้งจำนวนกรรมการแต่ละด้านที่จะเสนอให้มีการแต่งตั้ง รวมทั้งกำหนดกรอบระยะเวลาและวิธีการในการดำเนินการสรรหา เรียบร้อยแล้ว

ทั้งนี้ ภายหลังจากการประชุมดังกล่าวข้างต้น คณะกรรมการสรรหา ก็จักเริ่ม ดำเนินการสรรหาเพื่อให้ได้มาซึ่งบุคคลที่มีความรู้ความเชี่ยวชาญและความสามารถเป็นที่ประจักษ์ ในด้านที่กำหนดในคราวการประชุมครั้งที่ ๑/๒๕๖๗ ก่อนที่ฝ่ายเลขานุการจะดำเนินการรวบรวมรายชื่อ ตรวจสอบคุณสมบัติ ลักษณะต้องห้าม พร้อมทั้งประวัติและผลงานของผู้ได้รับการเสนอชื่อ เพื่อเสนอให้ คณะกรรมการสรรหา ดำเนินการพิจารณาคัดเลือกผู้ที่ได้รับการสรรหาเป็นกรรมการผู้ทรงคุณวุฒิ ในคราวการประชุมครั้งถัดไป

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบ ดังนี้

๑. รายงานความคืบหน้าการจัดทำ (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหา กรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.

๒. รายงานความคืบหน้าการสรรหาและแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

๓. รายงานความคืบหน้าการสรรหาและแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการ บริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

นายประเสริฐ จันทรรวงทอง ประธานกรรมการ มอบหมายให้ พลโท นรเศรษฐ์ พงษ์เจริญ ติดตามความคืบหน้าของการจัดทำระเบียบ เนื่องจากล่วงเลยมาเป็นระยะเวลานานพอสมควร

มติที่ประชุม รับทราบ ๑) รายงานความคืบหน้าการจัดทำ (ร่าง) ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหา กรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.

๒) รายงานความคืบหน้าการสรรหาและแต่งตั้งกรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการกำกับ ควบคุมดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และ ๓) รายงานความคืบหน้าการสรรหาและแต่งตั้ง กรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์

๓.๔ การเตรียมความพร้อมเข้าสู่ยุคควอนตัม

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขออนุญาตนำเรียนเพิ่มเติม เรื่องของควอนตัม คอมพิวเตอร์ที่จะนำความก้าวหน้าในด้านขีดความสามารถในด้านไอที และไซเบอร์ แต่ประเด็นที่จะนำเรียนทุกท่านต่อไป คือเรื่องของปัญหาของการถอดรหัสระบบรักษาความปลอดภัยต่าง ๆ ที่มีในปัจจุบันจะส่งผลกระทบจากการคาดการณ์เรื่องของการถอดรหัสนั้น ซึ่งอาจจะเกิดขึ้นใน ๕-๖ ปีข้างหน้า จึงมีความจำเป็นที่ประเทศไทยต้องมีความพร้อมในการเตรียมการล่วงหน้าในโอกาสยกระดับด้านความปลอดภัย เพื่อให้รับมือเรื่องของโอกาสที่ควอนตัมจะกระทบไซเบอร์ ทั้งนี้ขอมอบหมายให้พลอากาศตรี เฉลิมชัย วงษ์เกตุ ผู้อำนวยการศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ข้อกฎหมาย

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๒๒ บัญญัติว่า “สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” มีหน้าที่และอำนาจดังนี้

(๑๓) ศึกษาและวิจัยข้อมูลที่เป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

มาตรา ๓๖ บัญญัติว่า “เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” มีหน้าที่และอำนาจดังนี้

(๑) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและคณะกรรมการและข้อบังคับ นโยบาย มติ และประกาศของ กบส.

ข้อรายงาน

๑. ตามนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. ๒๕๖๑ – ๒๕๘๐) ได้กำหนดทิศทางการพัฒนาประเทศ ความท้าทายและโอกาสของประเทศไทย ในมิติภัยคุกคามไซเบอร์ โดยการจัดการกับภัยในรูปแบบใหม่ๆ รวมถึง ภัยคุกคามจากสารสนเทศรูปแบบต่างๆ มีการพัฒนาและเปลี่ยนแปลงรูปแบบอย่างต่อเนื่อง จึงต้องเตรียมความพร้อมเพื่อรับมือ เพิ่มขีดความสามารถของบุคลากรในการรักษาความมั่นคงปลอดภัยและการพัฒนาทักษะความรู้เพื่อป้องกันตนเองและหน่วยงาน ลดความเสี่ยงจากการถูกโจมตีหรือภัยคุกคามและลดความเสียหายจากผลกระทบที่อาจเกิดขึ้น ดังนั้น การเตรียมความพร้อมเข้าสู่ยุคควอนตัม จึงเป็นการดำเนินการเพื่อการสร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล เป็นบทบาทหน้าที่หลักของภาครัฐในการอำนวยความสะดวกให้กับทุกภาคส่วน ในการการรักษาความมั่นคงปลอดภัยไซเบอร์ ลดอุปสรรคเพิ่มประสิทธิภาพในการประกอบกิจกรรมที่เกี่ยวข้องต่างๆ พร้อมทั้งสร้างแนวทางขับเคลื่อนอย่างบูรณาการเพื่อรองรับการเติบโตของเทคโนโลยีดิจิทัลในอนาคต

๒. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจในการเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน จากสถานการณ์คอมพิวเตอร์แบบควอนตัมที่มี

ความสามารถในการถอดรหัสสูงกว่ายุคปัจจุบัน อาจส่งผลให้เกิดภัยคุกคามไซเบอร์เพิ่มมากขึ้น จึงจำเป็นต้องเสริมสร้างความรู้ความเข้าใจ และสร้างความตระหนักรู้ด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ เมื่อก้าวเข้าสู่ยุคควอนตัม

๓. สกมช. ได้เผยแพร่คำแนะนำแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม (Guidelines for Post-Quantum Readiness) ในเดือนธันวาคม ๒๕๖๖ เพื่อเสนอเป็นข้อมูลให้กับผู้ที่มีส่วนเกี่ยวข้องทุกภาคส่วนได้ร่วมพิจารณา และได้จัดประชุมเพื่อหารือแนวทางดำเนินการเตรียมความพร้อมสำหรับยุคควอนตัม ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนต่อไป

๔. เพื่อให้การเตรียมความพร้อมรับมือการก้าวเข้าสู่ยุคควอนตัมเป็นไปด้วยความเรียบร้อย และบรรลุตามวัตถุประสงค์ดังกล่าว สกมช. จึงมีความจำเป็นต้องอาศัยความร่วมมือจากผู้เชี่ยวชาญจากภายนอก เพื่อสนับสนุนข้อมูลที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์แบบควอนตัม รวมถึงดำเนินกิจกรรมต่างๆ เช่น การประชุมเชิงปฏิบัติการ การฝึกอบรมเชิงวิชาการและเชิงปฏิบัติการ ซึ่งที่ผ่านมา ได้มีการแต่งตั้งคณะทำงานดำเนินการเตรียมความพร้อมระบบสารสนเทศเพื่อเข้าสู่ยุคควอนตัม มาเพื่อดำเนินการในเรื่องดังกล่าวเป็นการเฉพาะ โดยมีองค์ประกอบ หน้าที่และอำนาจ ดังนี้

๑. องค์ประกอบ

- | | |
|---|--------------------------|
| ๑.๑ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | ที่ปรึกษาคณะทำงาน |
| ๑.๒ รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | ประธานคณะทำงาน |
| ๑.๓ ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คนที่ ๑ | รองประธานคณะทำงาน |
| ๑.๔ ผู้ช่วยเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คนที่ ๓ | คณะทำงาน |
| ๑.๕ ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | คณะทำงาน |
| ๑.๖ ผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ | คณะทำงาน |
| ๑.๗ ผู้แทนสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ | คณะทำงาน |
| ๑.๘ ผู้แทนสำนักงานพัฒนารัฐบาลดิจิทัล คณะทำงาน | |
| ๑.๙ นายจิรวัดน์ ตั้งปณิธานนท์ ศูนย์ความเป็นเลิศด้านฟิสิกส์
สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์
วิจัยและนวัตกรรม | คณะทำงาน |
| ๑.๑๐ นายณัฐวุฒิ กองสุววัฒน ศูนย์ความเป็นเลิศด้านฟิสิกส์
สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์
วิจัยและนวัตกรรม | คณะทำงาน |
| ๑.๑๑ ผู้อำนวยการศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ | คณะทำงาน
และเลขานุการ |

- | | | |
|------|--|-----------------------------------|
| ๑.๑๒ | ผู้อำนวยการฝ่ายวิเคราะห์และประมวลผลข้อมูล
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ | คณะทำงาน
และช่วยเหลืองานการ |
| ๑.๑๓ | ผู้อำนวยการฝ่ายวิจัยและพัฒนาเครือข่ายวิจัย
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ | คณะทำงาน
และผู้ช่วยเหลืองานการ |

๒. หน้าที่และอำนาจ

๒.๑ ศึกษา วิเคราะห์ข้อมูล หรือวิจัยในเรื่องที่เกี่ยวข้องกับเทคโนโลยีคอมพิวเตอร์แบบควอนตัม และแนวทางการดำเนินการเพื่อป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากคอมพิวเตอร์แบบควอนตัม

๒.๒ ประสานความร่วมมือกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานเอกชน และหน่วยงานต่างประเทศที่เกี่ยวข้อง

๒.๓ จัดประชุมเชิงปฏิบัติการเพื่อประยุกต์ใช้คำแนะนำแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม (Guidelines for Post-Quantum Readiness) กับหน่วยงานต้นแบบ

๒.๔ เผยแพร่ผลการศึกษา และฝึกอบรมเชิงวิชาการและเชิงปฏิบัติการ เพื่อส่งเสริมและผลักดันให้หน่วยงานของรัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานกำกับหรือดูแลเตรียมความพร้อมเข้าสู่ยุคควอนตัม

๒.๕ เชิญบุคคลมาร่วมประชุมหรือให้ข้อมูลที่เป็นประโยชน์ต่อการดำเนินการของคณะทำงานฯ

๒.๖ ประสานขอข้อมูลจากบุคคล และหน่วยงานต่างๆ ทั้งภาครัฐและเอกชนเพื่อประโยชน์ต่อการดำเนินงานของคณะทำงานฯ

๒.๗ เสนอต่อเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อแต่งตั้งคณะทำงานย่อยในการช่วยปฏิบัติงานของคณะทำงานได้ตามความจำเป็น

๒.๘ ปฏิบัติหน้าที่อื่นตามที่เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมอบหมาย

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบผลการดำเนินการเตรียมความพร้อมระบบสารสนเทศเพื่อเข้าสู่ยุคควอนตัมของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นายไพฑูรย์ อมรวิญญูเกียรติ กรรมการผู้ทรงคุณวุฒิด้านด้านกฎหมาย ขอเรียนต่อที่ประชุมเรื่องของควอนตัมเป็นเรื่องที่น่าสนใจ จากที่ สกมช. ได้ดำเนินการเห็นว่าปัจจัยที่ ตามที่ท่านวิเชฐ ตันติวานิช สอบถามว่า สกมช. ได้อันดับ ๗ จากทางด้านกฎหมาย ต้องชื่นชมประธานเพราะนอกจากกฎหมายทางไซเบอร์ในปีที่ผ่านมาท่านประธานได้ทำงานหนักมากในการควบคุมข้อมูลรั่วไหลของข้อมูลส่วนบุคคล ซึ่งกฎหมาย PDPA ครอบคลุมและส่งเสริมด้านความมั่นคงปลอดภัยไซเบอร์ ในปัจจัยที่ท่านเลขาชี้แจงมาจะเห็นได้ว่า เป็นผลจากกฎหมายทั้ง ๓ ฉบับ ทำให้ได้คะแนนสูง จากการหารือกับท่านวิเชฐฯ การที่เราแพ้เวียดนามเพราะ Organization ของเราเพิ่งเริ่มต้น และตามที่ฝ่ายเลขานุการนำเสนอเกี่ยวกับคณะทำงานเห็นว่าควรมีองค์ประกอบของคณะทำงานที่มาจากกฎหมาย เพราะองค์ประกอบในการดูแลควอนตัมเรื่องที่ใหม่ทั้งทางด้านเทคนิค และในส่วนของทางกฎหมายควรมีคนที่เข้าไปในเรื่องของการบังคับใช้กฎหมาย PDPA ที่มีความรัดกุมและเข้มแข็ง จึงขอเสนอในที่ประชุมและประธานให้แต่งตั้งที่ปรึกษาเพิ่มเติม โดยอาจจะมาจาก

คณะกรรมการผู้ทรงฯ ขอเสนอรายชื่อ ๑) นายไพบูลย์ อมรวิญญูเกียรติ ดูแลทางด้าน พ.ร.บ. ไซเบอร์ และ พ.ร.บ.คุ้มครอง พ.ร.บ.คอมพิวเตอร์ ๒) พันตำรวจเอก ญาณพล ยั่งยืน เป็นผู้ที่มีความเชี่ยวชาญกับทาง DSI อยู่แล้ว และ ๓) พลเอก มโน นุชเกษม ที่เกี่ยวข้องกับทางด้านการทหารหรือส่วนที่เกี่ยวข้องอื่น หรือผู้แทนจาก กระทรวงยุติธรรม และสำนักงานตำรวจแห่งชาติ ดังนั้น ควรให้ทางกฎหมายเข้าไปเรียนรู้ตั้งแต่แรก

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ขอรับฟังจากหลาย ๆ ท่าน เพื่อจะได้ข้อสรุปครั้งเดียว ท่านไพบูลย์ฯ ได้เสนอให้มีการตั้งที่ปรึกษาเป็นที่ปรึกษาเพิ่มเติมใช้ใหม่ เขาเป็นองค์ประกอบของคณะทำงานชุดนี้ ประธานรับทราบไม่ขัดข้องและน่าจะเป็นประโยชน์ด้วย โดยให้เสนอชื่อในการประชุมครั้งนี้

พลเรือเอก สุพัตต์ ยุทธวงศ์ รองปลัดกระทรวงกลาโหม ผู้แทนจากรัฐมนตรีว่าการกระทรวงกลาโหม ขอเสนอต่อที่ประชุม กระทรวงกลาโหมมีหน่วยงานที่ดูแลเกี่ยวกับเรื่องเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ทางกรมเทคโนโลยีสารสนเทศและอวกาศกลาโหมเป็นหน่วยงานโดยเฉพาะของกระทรวงกลาโหมที่ดูแลทั้งหมด ถ้าจะจัดหาผู้แทนจากกระทรวงกลาโหมก็สามารถหาได้จากหน่วยงานเหล่านี้

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ขอเสนอเพิ่มเติมที่ปรึกษาสองท่าน มีท่านนายไพบูลย์ อมรวิญญูเกียรติกับพันตำรวจเอก ญาณพล ยั่งยืน และฝ่ายกระทรวงกลาโหมเป็นจำนวน ๓ ท่านเป็นที่ปรึกษาเพิ่มเติมจากท่านอมรฯ เดิมมีอยู่แค่ท่านเดียว

นางสาวตรุณี พิกุลทอง ขอเสนอนายปภาสิต เหลืองทอง ดำรงตำแหน่งกรรมการผู้ทรงด้านกฎหมายของกกม. ขอนำเสนอขึ้นมาเป็นคณะกรรมการฯ ทำงานชุดนี้ด้วย

พลตำรวจตรี ชูศักดิ์ ขนาคณิต ผู้บังคับการ กองบังคับการตรวจสอบและวิเคราะห์ ผู้แทนผู้บัญชาการตำรวจแห่งชาติ ขอเสนอต่อที่ประชุมดังนี้ ต่อไปในอนาคตจะมีคดีอาชญากรรมเทคโนโลยีที่มีการใช้ควอนตัมเข้ามากระทำผิดมากขึ้น อยากให้เพิ่มของในส่วนของการตำรวจเข้ามาไปด้วย เพราะคิดว่าจะได้มีผู้เชี่ยวชาญที่มีความรู้ด้านนี้แล้วก็นำไปสื่อสารกับเจ้าหน้าที่ตำรวจได้

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ขอสอบถามว่าจะใช้คำว่าผู้แทนจากสำนักงานตำรวจแห่งชาติอย่างนั้นเรียกว่าจะตั้งเกี่ยวกับฝ่ายเทคโนโลยีสารสนเทศ ท่านมีความเห็นอย่างไร

พลตำรวจตรี ชูศักดิ์ ขนาคณิต ผู้บังคับการ กองบังคับการตรวจสอบและวิเคราะห์ ผู้แทนผู้บัญชาการตำรวจแห่งชาติ ชี้แจงเพิ่มเติมว่า ขอให้ใช้คำว่า “ผู้แทน”

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี รับไปดำเนินการประสานงานประกอบด้วยฝ่ายกระทรวงกลาโหม ฝ่ายสำนักงานตำรวจแห่งชาติ และที่ปรึกษาที่ตั้งเพิ่มเติม และนายปภาสิต เหลืองทอง กรรมการผู้ทรงด้านกฎหมายของ กกม.

นายไตรยฤทธิ์ เตมหิวงศ์ รองปลัดกระทรวงยุติธรรม ผู้แทนปลัดกระทรวงยุติธรรม ขอเสนอเพิ่มเติมดังนี้ ตามที่ท่านไพบูลย์ฯ ได้อ้างถึงมิติของกฎหมาย ในมุมของกระทรวงยุติธรรมที่จะเป็นประโยชน์ได้ก็คือช่วยคดีเรื่องของกฎหมาย ซึ่งตรงนี้จะมิกองของกฎหมาย ปัจจุบันได้พิจารณา พ.ร.บ. มากมาย ที่สนับสนุนรัฐบาล เช่น พ.ร.บ. สมรสเท่าเทียม เป็นต้น ทั้งนี้ กระทรวงยุติธรรมพร้อมสนับสนุนการดำเนินการของ สกมช.

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี กล่าวสรุปว่า ที่ประชุมเห็นชอบตามที่ได้เพิ่มเติมเข้ามา ส่วนจะเป็นใครมอบหมายเลขานุการประสานงาน และจะใช้เป็นชื่อ หรือเป็นผู้แทน แล้วในวาระนี้ที่ประชุม รับทราบแล้วก็ได้ให้ความเห็นให้เพิ่มองค์ประกอบในคณะทำงานขึ้นมาตามที่ที่ประชุมให้ความเห็น

มติที่ประชุม รับทราบผลการดำเนินการเตรียมความพร้อมระบบสารสนเทศเพื่อเข้าสู่ยุคควอนตัมของสำนักงานคณะกรรมการการรักษความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมอบหมายฝ่ายเลขานุการปรับปรุงองค์ประกอบคณะทำงานฯ ตามที่ที่ประชุมให้ความเห็น

๓.๕ ความคืบหน้าการดำเนินงานตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง

พลอากาศตรี อมร ชมเชย เลขานุการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมพันโท ญาณินทร์ สุรพันธ์ไพโรจน์ ผู้อำนวยการฝ่ายขับเคลื่อนยุทธศาสตร์ประเทศ สำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ฐานอำนาจ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙(๙) บัญญัติว่า “คณะกรรมการมีหน้าที่และอำนาจ ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้”

มาตรา ๔๓ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

มาตรา ๕๓ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

ความเป็นมา

หน้าที่และอำนาจของสำนักงานตามมาตรา ๒๒ (๗) ในการดำเนินการปฏิบัติ การประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผน ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของ กมช. ทั้งนี้ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานควบคุมหรือกำกับดูแล (Regulator), หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน CII) และ หน่วยงานของรัฐ (GA) มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ข้อรายงาน

การประชุม กมช. ครั้งที่ ๑ ประจำปี พ.ศ. ๒๕๖๗ เมื่อวันที่ ๒๕ มีนาคม ๒๕๖๗ ที่ผ่าน มานั้น ที่ประชุมมีมติเห็นชอบให้ สกมช. เร่งรัดการติดตามการดำเนินงานตาม พ.ร.บ.การรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และรายงานผลการดำเนินการต่อ ประธาน กมช. รับทราบเป็นระยะ นั้น

สกมช. ขอรายงานผลการดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัย ไซเบอร์ พ.ศ. ๒๕๖๒ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ รายละเอียดดังนี้

ลำดับ	การดำเนินงาน	ผลการดำเนินงาน		หมายเหตุ
		Regulator (๑๙ หน่วย)	หน่วยงาน CII (๖๑ หน่วย)	
๑	นโยบายและแผนปฏิบัติการว่า ด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์	๑๙	๖๑	
๒	การจัดทำประมวลแนวทางปฏิบัติ ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์	๑๕	๖๑	
๓	การดำเนินการตรวจสอบ มาตรฐานขั้นต่ำ	๑๔	-	(เฉพาะ Regulator)
๔	การดำเนินการตามมาตรา ๕๔	-	๕๙	(เฉพาะหน่วยงาน CII)

ฝ่ายเลขานุการขอนำเสนอต่อที่ประชุมเพื่อทราบความคืบหน้าการดำเนินงานตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ขอให้คณะกรรมการให้ความเห็นเกี่ยวกับการ ปฏิบัติตาม พ.ร.บ. ฉบับนี้ กรณีผู้ไม่ปฏิบัติตาม พ.ร.บ. มีความผิดอย่างไร

นายไพบุลย์ อมรวิญญูเกียรติ กรรมการผู้ทรงคุณวุฒิฯ ได้นำเรียนที่ประชุมว่ากฎหมาย ฉบับนี้มีรู้รั่วเพราะกฎหมายบังคับใช้กับ CII หรือ หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ ข้อมูลที่รั่วจาก

หน่วยงานรัฐและเอกชนต่าง ๆ ที่ไม่ได้เป็น CII ไม่สามารถปรับอะไรไม่ได้เลย ซึ่งเป็นปัญหาใหญ่ ต้องอาศัย PDPA มาช่วย ในส่วนนี้ควรรับแก้ไขเฉพาะการประกาศ CII ยังมีช่องว่างที่ทำให้ภาครัฐและเอกชนไม่ยอมเป็น CII เพราะรู้ว่าเราบังคับเขาไม่ได้

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ชี้แจงเพิ่มเติมว่า พ.ร.บ. ไซเบอร์ กำหนดให้หน่วยงานที่ไม่ทำตาม พ.ร.บ. สกมช.ทำได้เพียงสรุปนำเรียนท่านนายกฯ ให้พิจารณาต่อไป เพราะฉะนั้นจะไม่เหมือนกับ พ.ร.บ. PDPA ที่มีบทลงโทษทั้งจำทั้งปรับที่เป็นตัวเลขที่ชัดเจน ดังนั้นการปรับปรุง พ.ร.บ. จะต้องเสริมมาตรการในเรื่องของการลงโทษที่ชัดเจนมากขึ้น

นางสาวตรุณี พิกุลทอง ผู้อำนวยการสำนักกฎหมาย ให้ความคิดเห็นเพิ่มเติมว่า มีในส่วน ของบทบังคับ CII อย่างเช่นกรณีที่เกิดภัยคุกคามทางไซเบอร์อย่างร้ายแรงตามมาตรา ๕๗ ของ พ.ร.บ.ไซเบอร์ CII ไม่แจ้งจะต้องถูกปรับ ในอัตราไม่เกิน ๒๐๐,๐๐๐ บาท หรือกรณีที่เราขอข้อมูลไปยังหน่วยงานถ้าไม่ให้ความร่วมมือจะต้องถูกปรับไม่เกิน ๑๐๐,๐๐๐ บาท เป็นต้น

นายปริญญา หอมเอนก กรรมการผู้ทรงคุณวุฒิฯ ให้ความคิดเห็นเพิ่มเติมว่าปัจจุบันการเป็น หน่วยงาน CII จะต้องสมัครใจเป็น CII ควรปรับปรุงกฎหมายให้สามารถกำหนดหน่วยงานที่ควรเป็น CII ได้เช่น ธนาคาร พาณิชย์ทุกธนาคาร ภายใต้ ธปท. เป็น CII

พันตำรวจเอก ญาณพล ยั่งยืน กรรมการผู้ทรงคุณวุฒิฯ ให้ความคิดเห็นเพิ่มเติมว่า เห็นควรต้องปรับปรุงกฎหมายกรณีการจัดตั้ง CII แล้วอาจจะต้องมีการกำหนดเป็นกลุ่มหรือประเภทครอบคลุม ได้มากขึ้น โดยไม่ต้องตี ตัวอย่างเช่น สหกรณ์มีเงินเยอะกว่าธนาคารไม่อยู่ในความดูแลของ ธปท. ตลอดจน ปัญหาเกี่ยวกับเรื่องการเบิกเงิน รับเงิน ของ สกมช. รับเงินต้องส่งคลังทั้งหมด ในส่วนนี้ต้องได้รับการแก้ไข

นายไพบุลย์ อมรภิญโญเกียรติ กรรมการผู้ทรงคุณวุฒิฯ ให้ความคิดเห็นเพิ่มเติมว่า ปัจจุบันฝ่าย เลขานุการ ได้ร่างแก้ไขหน่วยงาน CII ให้รวมถึงเอกชน เช่น ผู้ให้บริการ cloud security ที่เข้ามาให้บริการ ข้อมูลจำนวนเยอะในตัวร่างประกาศใหม่ควรกำหนดให้เป็น CII เพราะต่างประเทศจะให้ประกาศเป็น CII เฉพาะกิจ ไม่ให้ถูกแท็กด้วยตัวล่างใหม่ค่อนข้างจะตอบเจตนาในทำงานได้มากขึ้น ก็เสนอให้เร่งปรับปรุงทำให้ มาตรา ๔๙ ครอบคลุมมากขึ้น เด็ดขาดทำงานง่ายขึ้น

นายวิเชฐ ตันติวานิช กรรมการผู้ทรงคุณวุฒิฯ ขออนุญาตเสนอความเห็นที่กรณีกฎหมายแก้แล้วซ้ำ ด้านการเงินยังมีการกำกับโดยตลาดหลักทรัพย์ หากประธาน นายพิชัย นริพทะพันธุ์ รัฐมนตรีว่าการ กระทรวงการคลัง ใช้กลไกผ่านระเบียบของตลาดหลักทรัพย์ โดยขอความร่วมมือ หากไม่ปฏิบัติก็ไม่ได้ Score ที่ดี เพื่อสามารถเริ่มทำงานได้ก่อน

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี รับทราบว่ามีกระบวนการความคืบหน้าในการ ดำเนินการตาม พ.ร.บ. และมอบหมายฝ่ายเลขานุการพิจารณาข้อเสนอแนะของคณะกรรมการในเรื่องของการ ปรับปรุงกฎหมายให้สามารถบังคับใช้ได้เกิดประโยชน์สูงสุด

มติที่ประชุม รับทราบความคืบหน้าการดำเนินงานตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง และมอบหมายฝ่ายเลขานุการพิจารณา ข้อเสนอแนะของคณะกรรมการในเรื่องของการปรับปรุงกฎหมายให้สามารถบังคับใช้ได้เกิด ประโยชน์สูงสุด

๓.๖ ความคืบหน้าการบูรณาการการส่งเสริมและผลักดันการขับเคลื่อนโครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุงแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. ๒๕๖๖ – ๒๕๗๐

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษามันคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมพันโท ญาณินทร์ สุรพันธ์ไพโรจน์ ผู้อำนวยการฝ่ายขับเคลื่อนยุทธศาสตร์ประเทศ สำนักนโยบายยุทธศาสตร์การรักษามันคงปลอดภัยไซเบอร์ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ฐานอำนาจ

พระราชบัญญัติการรักษามันคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙(๖) บัญญัติว่า “คณะกรรมการมีหน้าที่และอำนาจ กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษามันคงปลอดภัยไซเบอร์”

มาตรา ๒๒(๑๒) บัญญัติว่า “สภมช. มีหน้าที่และอำนาจ เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษามันคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ”

ความเป็นมา

การขับเคลื่อนแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. ๒๕๖๖-๒๕๗๐ เป็นสิ่งที่มุ่งสนับสนุนให้ครอบครัวและชุมชนสามารถส่งเสริมให้เด็กและเยาวชนมีความเป็นอยู่ที่ดีผ่านงานเชิงป้องกันทางเศรษฐกิจ สังคม และสุขอนามัย โดยทำงานร่วมกับชุมชนและครอบครัวในการสนับสนุนเด็กและครอบครัวที่ต้องการความช่วยเหลือ โดย สภมช. ให้ความสำคัญในการบูรณาการร่วมกับหน่วยงานที่เกี่ยวข้องในการกำหนดให้มี “มาตรฐานและแนวปฏิบัติระหว่างหน่วยงานภาครัฐและภาคเอกชน เพื่อกำกับดูแลให้เกิดพื้นที่ปลอดภัยสำหรับเด็กทั้งทางกายภาพและทางออนไลน์” และสอดคล้องกับนโยบายของรัฐบาลชุดปัจจุบันที่ให้ความสำคัญในการแก้ปัญหาอาชญากรรมออนไลน์/มิจฉาชีพ และอาชญากรรมข้ามชาติ รวมถึงการส่งเสริมการเติบโตอย่างมีคุณภาพของเด็กทุกคนอย่างเท่าเทียมในการพัฒนาทักษะวิทยาศาสตร์ เทคโนโลยี และการคิดวิเคราะห์อย่างมีเหตุผล

ข้อรายงาน

สภมช. มีการดำเนินงานที่สำคัญในการขับเคลื่อนร่วมกับหน่วยงานที่เกี่ยวข้องจัดการประชุมจำนวน ๓ ครั้ง ดังนี้

ครั้งที่ ๑ การประชุมเพื่อกำหนดแนวทางการขับเคลื่อนกิจกรรมภายใต้ร่างแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. ๒๕๖๖-๒๕๗๐ เมื่อวันที่ ๒ สิงหาคม ๒๕๖๗

ครั้งที่ ๒ การประชุมเชิงปฏิบัติการ “การระดมสมองพัฒนา มาตรฐานและแนวปฏิบัติระหว่างหน่วยงานภาครัฐและภาคเอกชน เพื่อกำกับดูแลให้เกิดพื้นที่ปลอดภัยสำหรับเด็กทั้งทางกายภาพและออนไลน์” เมื่อวันที่ ๖ สิงหาคม ๒๕๖๗

และ ครั้งที่ ๓ การประชุมสรุปทบทวนหลังการดำเนินการภายใน สภมช. และหน่วยงานที่เกี่ยวข้อง เมื่อวันที่ ๑๕ สิงหาคม ๒๕๖๗

โดยมีวัตถุประสงค์หลักเพื่อยกระดับแนวทางการสร้างกลไกการปกป้องคุ้มครองเด็กและเยาวชนในการใช้สื่อออนไลน์ และร่วมกันบูรณาการหน่วยงานทุกภาคส่วนเพื่อกำหนดเป็น (ร่าง) มาตรฐานและ

แนวปฏิบัติระหว่างหน่วยงานภาครัฐและภาคเอกชน เพื่อกำกับดูแลให้เกิดพื้นที่ปลอดภัยสำหรับเด็กทั้งทางกายภาพและออนไลน์ซึ่งจะเป็นแนวทางในการขับเคลื่อนกิจกรรมต่างๆ ที่เกี่ยวข้องภายใต้ร่างแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. ๒๕๖๖-๒๕๗๐

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบความคืบหน้าการบูรณาการการส่งเสริมและผลักดันการขับเคลื่อนโครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุงแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. ๒๕๖๖ - ๒๕๗๐

มติที่ประชุม รับทราบความคืบหน้าการบูรณาการการส่งเสริมและผลักดันการขับเคลื่อนโครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุงแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. ๒๕๖๖ - ๒๕๗๐

๓.๗ รายงานผลทบทวนการดำเนินการตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมพันตำรวจเอก ฉันทกฤษ พรหมจันทร์ ผู้อำนวยการสำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ความเป็นมา

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลในแต่ละด้านพิจารณาความเหมาะสมในการกำหนดแนวทางพิจารณาให้ภารกิจหรือบริการของหน่วยงานที่อยู่ภายใต้การดูแลของตนเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้รายละเอียดของลักษณะหน่วยงานที่มีภารกิจหรือบริการตามที่กำหนดไว้ในแนบท้ายประกาศนี้ และให้แจ้งต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อทราบต่อไป

ข้อรายงาน

สกมช. ได้ดำเนินการจัดส่งหนังสือเพื่อแจ้งทบทวนการดำเนินการตาม มาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบด้วย

การทบทวนการดำเนินการตามมาตรา ๔๙

สกมช. ได้มีหนังสือ ที่ สกมช ๐๖๐๐/ว๒๗ ลงวันที่ ๙ มกราคม ๒๕๖๗ เรื่อง ขอให้หน่วยงานแจ้งหรือทบทวนการดำเนินการ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๔ ไปยังหน่วยงานควบคุมหรือกำกับดูแล (Regulator) จำนวน ๑๙ หน่วยงาน โดยสรุปสถานะการดำเนินการได้ ดังนี้ (ข้อมูล ณ วันที่ ๓ ตุลาคม ๒๕๖๗)

๑.๑ หน่วยงานที่ตอบกลับแล้ว จำนวน ๑๙ หน่วยงาน

๑.๒ หน่วยงานควบคุมหรือกำกับดูแล (Regulator) ขอเพิ่มเติมหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบด้วย

๑.๒.๑ สำนักงานการบินพลเรือนแห่งประเทศไทย

- ขอเพิ่มหน่วยงาน CII จำนวน ๑๐ หน่วยงาน ดังนี้

๑. กองการบินทหารเรือ (หอบังคับการบิน แผนกบังคับการบิน กองปฏิบัติการฐานบินสถานีการบิน)
๒. บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
๓. การท่าอากาศยานอุตะภา
๔. บริษัท การบินกรุงเทพ จำกัด (มหาชน)
๕. บริษัท เอซี เอวิเอชั่น จำกัด
๖. บริษัท แอ็ดวานซ์ เอวิเอชั่น เจ็ท จำกัด
๗. บริษัท สายการบินนกแอร์ จำกัด (มหาชน)
๘. บริษัท ไทยเวียตเจ็ทแอร์ จำกัด
๙. บริษัท ดับบลิวเอฟเอสฟิจีคาร์โก จำกัด
๑๐. บริษัท เอ็มเจ็ท จำกัด

๑.๓ ปัจจุบันหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีจำนวนทั้งสิ้น

๗๓ หน่วยงาน

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบรายงานสรุปผลการทบทวนการดำเนินการตาม มาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นายรัชกรณ นภาพรพิพัฒน์ ผู้แทนเลขาธิการสภาความมั่นคงแห่งชาติ เข้าใจว่าวาระนี้เป็นเพื่อทราบจากการติดตามหน่วยงานที่ทำหน้าที่ควบคุมกำกับดูแล (Regulator) ที่มีการปรับเปลี่ยนให้เร็วขึ้นเพื่อเป็นการปรับการทำงานให้กับ CII ด้านอื่น ๆ ด้วย เช่น ด้านความมั่นคงมีหนังสือไปถึงบอร์ดเรียบร้อยแล้ว ในชุดนี้เร่งรัดส่วนเรื่องซีเทค เป็นการกำกับดูแลของสหประชาชาติเรื่องของไซเบอร์ต่าง ๆ โจมตีการก่อการร้ายต่าง ๆ ซึ่งจะรายงานผลมาทาง สมช. จะรายงานให้กับทาง สกมช. เรียบร้อยแล้ว ควรจะมีข้อพิจารณาในการปรับปรุงอะไรบ้าง นั้นจะเป็นมิติการก่อการร้ายไซเบอร์แท้ก็ ไซเบอร์คราม ต่างๆ

นายไพบุลย์ อมรภิญโญเกียรติ กรรมการผู้ทรงคุณวุฒิฯ ให้ข้อสังเกตว่า กรณีการบินไทยยังไม่เป็น CII ซึ่งเป็นสายการบินแห่งชาติ ที่มีข้อมูลคนไทยอยู่เป็นจำนวนมาก หากมีปัญหาในเรื่องของภัยคุกคามทางไซเบอร์ เราจะไม่สามารถทำอะไรได้ จึงอยากขอข้อมูลเพิ่มเติม

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ให้ข้อมูลเพิ่มเติมว่า ปัจจุบัน สำนักงานการบินพลเรือนซึ่งเป็น Regulator ประสานงานกับหน่วยงานว่าพร้อมเป็น CII หรือไม่ ฝ่ายเลขานุการขอรับไปประสาน กับหน่วยงานที่เกี่ยวข้องทั้งในส่วนของสำนักงานการบินพลเรือนและในส่วนของสายการบินไทยเพื่อยกระดับและขับเคลื่อนต่อไป

นายรัชกรณ นภาพรพิพัฒน์ ผู้แทนเลขาธิการสภาความมั่นคงแห่งชาติ ขออนุญาตอันนี้เป็น การตรวจโดยสหประชาชาติ ทาง สมช. ได้ แจ้งหน่วยโดยตรง แล้วเพื่อปรับปรุงแก้ไขตามมาตรฐานต่าง ๆ ที่หน่วยงานคาดหวังไว้ ทั้งหมดขึ้นอยู่กับความพร้อมของประเทศไทยพยายามเข้าไปในทางสากลให้ถึง เช่น การฟอกเงิน อีกส่วนหนึ่งที่ท่านอมรนำเรียน เป็นของ Regulator ความพร้อมของ CII

นายวิเชฐ ตันติวานิช กรรมการผู้ทรงคุณวุฒิฯ ให้ความเห็นว่ากรณีนี้ควรมีการผลักดันคล้ายกับตลาดหลักทรัพย์ คือ TG เป็น Regulator อยู่ ให้เขาเฝ้าฟอร์ชเข้ามาทุกคนจะร่วมมือ

นายไพบุลย์ อมรวิญญูเกียรติ การบินไทยที่ผมรู้ข้อมูลรั่วไหลเยอะมากและมีบริษัทในเครือจำนวนมาก ข้อมูลของคนไทยอยู่จำนวนมาก ผมเลยเป็นกังวลเรื่องของไซเบอร์มากสมมติว่าถ้าเกิดภัยคุกคามในระดับร้ายแรงแต่เราจะบังคับเขาไม่ได้เพราะเขาไม่ใช่ CII ก็ลำบาก PDPA ขาดเดียวและจะกลายเป็นว่าทีมสมช. ทำงานลำบาก ขอแจ้งเป็นข้อสังเกต

นายประเสริฐ จันทรวงทอง รองนายกรัฐมนตรี รับทราบและมอบหมายให้ฝ่ายเลขานุการไปประสานงานให้การบินไทยซึ่งเป็นสายการบินหลักเข้าร่วม

มติที่ประชุม รับทราบรายงานสรุปผลการทบทวนการดำเนินการตาม มาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และการดำเนินการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมอบหมายให้ฝ่ายเลขานุการไปประสานงานให้การบินไทยซึ่งเป็นสายการบินหลักเข้าร่วม

๓.๘ การประกาศเกียรติคุณรางวัลเลิศรัฐ ประจำปี ๒๕๖๗ ในรางวัลบริการภาครัฐประเภทนวัตกรรมบริการ กับผลงาน Proactive Protection X Total defense by NCSA"

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมพลอากาศตรี วุฒิภัทร จันทรสาร ผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ฐานอำนาจ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ความเป็นมา

หนังสือสำนักงาน ก.พ.ร. ที่ นร ๑๒๐๖/๕๐๕๓ ลงวันที่ ๗ ธันวาคม ๒๕๖๖ เรื่อง การชี้แจงแนวทางการสมัครและหลักเกณฑ์การพิจารณารางวัลเลิศรัฐ ประจำปี ๒๕๖๗ โดยสำนักงาน ก.พ.ร. ดำเนินการรับสมัครรางวัลเลิศรัฐประจำปี ๒๕๖๗ เพื่อเตรียมความพร้อม รวมถึงสร้างความรู้ความเข้าใจให้แก่หน่วยงานภาครัฐที่มีความประสงค์จะสมัครขอรับรางวัลเลิศรัฐ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ส่งผลงานจำนวน ๓ ผลงาน ในรางวัลบริการภาครัฐ ประเภทนวัตกรรมบริการ ด้วยผลงานของสำนักปฏิบัติการชื่อผลงาน Proactive Protection X Total defense by NCSA และประเภทบูรณาการข้อมูลในรูปแบบดิจิทัล ด้วยผลงานของสำนักประสานงาน ชื่อผลงาน โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ MISIP) และรางวัลบริหารราชการแบบมีส่วนร่วม ประเภทเปิดใจใกล้ชิดประชาชน ด้วยผลงานของสำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ชื่อผลงาน “กิจกรรมยกระดับมาตรฐาน cybersecurity สำหรับหน่วยงาน เพื่อบริการประชาชน”

ข้อรายงาน

ตามประกาศคณะกรรมการพัฒนาระบบราชการ เรื่อง ผลการพิจารณารางวัลเลิศรัฐ ประจำปี ๒๕๖๗ ประกาศ ณ วันที่ ๓ กันยายน ๒๕๖๗ คณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) ได้มีมติมอบรางวัลให้กับหน่วยงานที่มีผลการดำเนินการที่เป็นเลิศทั้งในด้านการเพิ่มประสิทธิภาพการให้บริการภาครัฐ การพัฒนาคุณภาพการบริหารจัดการภาครัฐและเปิดระบบราชการให้ภาคส่วนอื่นเข้ามามีส่วนร่วม และสำนักงาน ก.พ.ร. ได้มีหนังสือสำนักงาน ก.พ.ร. ที่ นร ๑๒๐๖/๒๖๒๑ ลงวันที่ ๖ กันยายน ๒๕๖๗ เรื่อง ขอเชิญร่วมงานเสวนาวิชาการและพิธีมอบรางวัลเลิศรัฐ ประจำปี ๒๕๖๗ โดยได้เชิญเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และผู้แทน สกมช. เข้ารับรางวัลบริการภาครัฐ ประเภทนวัตกรรมบริการ กับผลงาน Proactive Protection X Total defense by NCSA ซึ่งเมื่อวันที่ ๑๘ กันยายน ๒๕๖๗ นำโดย พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พันตำรวจเอก ฉันทกฤษ พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ (ตำแหน่ง ณ ขณะนั้น) และผู้ปฏิบัติงาน สกมช. เข้าร่วมพิธีมอบรางวัลเลิศรัฐ ประจำปี ๒๕๖๗ ณ ห้องรอยัล จูบิลี บอลรูม อาคารชาเลนเจอร์ อิมแพคเมืองทองธานี ทั้งนี้ ในปีงบประมาณถัดไปจะพัฒนาผลงานเพื่อเข้าร่วมสมัครรางวัลเลิศรัฐในสาขาอื่น ๆ อันเป็นเกียรติประวัติในการรับรองการดำเนินงานเชิงประจักษ์ของ สกมช. ต่อไป

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบการประกาศเกียรติคุณรางวัลเลิศรัฐ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ในรางวัลบริการภาครัฐ ประเภทนวัตกรรมบริการ กับผลงาน Proactive Protection X Total defense by NCSA

ประธานกล่าวขอแสดงความยินดีด้วยในการทำงานแบบ Proactive Protection ถือว่าเป็นการประกาศเกียรติคุณที่ประชุมรับทราบ

มติที่ประชุม รับทราบการประกาศเกียรติคุณรางวัลเลิศรัฐ ประจำปีงบประมาณ พ.ศ. ๒๕๖๗ ในรางวัลบริการภาครัฐ ประเภทนวัตกรรมบริการ กับผลงาน Proactive Protection X Total defense by NCSA

๓.๙ รายงานผลการลงนามบันทึกความเข้าใจด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมพลอากาศตรี วุฒิภัทร จันทรสาร ผู้อำนวยการสำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

๓.๙.๑ การลงนามบันทึกความเข้าใจด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓.๙.๑.๑ รายงานผลการลงนามบันทึกข้อตกลงความร่วมมือในการจัดทำพร้อมทั้งเผยแพร่สื่อประชาสัมพันธ์ ภายใต้โครงการ “Digital Vaccine” ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ ๑๒ หน่วยงาน

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย สธ.กมช. ได้จัดพิธีลงนามบันทึกข้อตกลงความร่วมมือในการจัดทำพร้อมทั้งเผยแพร่สื่อประชาสัมพันธ์ภายใต้โครงการ “Digital Vaccine” ร่วมกับ ๑๑ หน่วยงาน ได้แก่ ๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ๒) สำนักงานตำรวจแห่งชาติ ๓) กรมสอบสวนคดีพิเศษ ๔) กรมประชาสัมพันธ์ ๕) ธนาคารแห่งประเทศไทย ๖) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ ๗) สำนักงานป้องกันและปราบปรามการฟอกเงิน ๘) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ๙) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ๑๐) สมาคมธนาคารไทย และ ๑๑) สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ เมื่อวันที่ ๙ สิงหาคม พ.ศ. ๒๕๖๗

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมเพื่อทราบผลการดำเนินการรายงานผลการลงนามบันทึกความเข้าใจว่าด้วยความร่วมมือของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อเมื่อวันที่ ๙ สิงหาคม พ.ศ. ๒๕๖๗ จำนวน ๑๒ หน่วยงาน ดังนี้

- ๑) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- ๒) สำนักงานตำรวจแห่งชาติ
- ๓) กรมสอบสวนคดีพิเศษ
- ๔) กรมประชาสัมพันธ์
- ๕) ธนาคารแห่งประเทศไทย
- ๖) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
- ๗) สำนักงานป้องกันและปราบปรามการฟอกเงิน
- ๘) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- ๙) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- ๑๐) สมาคมธนาคารไทย
- ๑๑) สมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์

พลตำรวจตรี ชูศักดิ์ ขนาดนิต ผู้แทนจากสำนักงานตำรวจแห่งชาติ ถือว่าเป็นโครงการที่ดีมากการทำวัคซีนไซเบอร์ จากที่สำนักงานตำรวจฯ เคยทำมาหลายปีแล้ว เมื่อครั้งท่านดำรงศักดิ์ซึ่งอาจารย์ปริญญาฯ ไปให้คำปรึกษา ซึ่งตอนนั้นจะมีความเข้มแข็งและมีการแถลงข่าวทุกอาทิตย์รูปแบบกระทำผิดทำแบบไหนและวิธีการป้องกันตัวเองทำอะไรซึ่งก็ทำให้ จากการดูสถิติการทำความผิดจะลดลงแต่ช่วงหลังสำนักงานตำรวจแห่งชาติอาจจะดูลดลงไปเพราะท่านเกษียณแล้ว ส่วน ผบ.ตร. รอคอยใหม่อาจจะยังไม่เข้าใจอาชญากรรมทางไซเบอร์เท่าไร โดยอาศัยอาจารย์ปริญญาฯ เป็นที่ปรึกษา ทั้งนี้ อาจารย์ให้คำปรึกษามากทำให้มีมาตรการเด่นวัคซีนไซเบอร์อย่างเข้มแข็งอยากให้ทาง สกมช. ดำเนินการอย่างต่อเนื่อง ทางสำนักงานตำรวจฯ ก็มีโครงการนี้อย่างต่อเนื่องเหมือนกันแต่ยังไม่เข้มแข็งเหมือนเดิมแต่ก็จะพยายามทำให้ดีที่สุดช่วงนี้เราก็จะมีให้ ประชาชน ทำคลิป เกี่ยวกับอาชญากรรม เข้าประกวด เพื่อรับรางวัลจากสำนักงานตำรวจฯ

มติที่ประชุม รับทราบรายงานผลการลงนามบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๓.๙.๒ ผลการการดำเนินงานเสริมสร้างความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จากการลงนามบันทึกความร่วมมือระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับหน่วยงานต่าง ๆ

ผลการการดำเนินงานเสริมสร้างความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จากการลงนามบันทึกความร่วมมือ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ หน่วยงานต่าง ๆ

๓.๙.๒.๑ กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.)

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย ลธ.กมช. และกองทุนเงินให้กู้ยืมเพื่อการศึกษา โดย นายชัยณรงค์ กัจฉปานันท์ ผู้จัดการกองทุนเงินให้กู้ยืมเพื่อการศึกษา ได้มีการลงนามในบันทึกความเข้าใจว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ กองทุนเงินให้กู้ยืมเพื่อการศึกษา เมื่อวันที่ ๑๗ มกราคม ๒๕๖๗ ณ ห้องประชุม Confidential ชั้น ๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นที่เรียบร้อยแล้ว และได้ดำเนินงานร่วมกัน ดังนี้

๑. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยพลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ นายชัยณรงค์ กัจฉปานันท์ ผู้จัดการกองทุนเงินให้กู้ยืมเพื่อการศึกษา พร้อมด้วยนางสายชล ทรัพย์มากอุดม หัวหน้าหน่วยธุรกิจประชาสัมพันธ์และงานธุรกิจสัมพันธ์ AIS ร่วมภารกิจสร้างภูมิคุ้มกันไซเบอร์ เดินหน้าขยายผลการเรียนรู้หลักสูตรอุ่นใจไซเบอร์หลักสูตรการเรียนรู้ด้านทักษะดิจิทัลที่ได้รับรองจากกระทรวงศึกษาธิการให้เป็นไปตามมาตรฐานของหลักสูตรการศึกษาไทยไปยังนักเรียนระดับมัธยมปลายสายสามัญ สายอาชีพ กลุ่มอาชีวศึกษา และนักศึกษาในระดับอุดมศึกษาผู้กู้ยืม เพื่อให้เยาวชนไทยได้เรียนรู้การป้องกัน รับมือ หรือแม้แต่การลดความเสี่ยงจากการใช้งานดิจิทัลที่อาจมีภัยคุกคามทางไซเบอร์แฝงมาในทุกรูปแบบ พร้อมทั้งได้สะสมชั่วโมงจิตสาธารณะได้ ๓ ชั่วโมง

๒. วันอังคารที่ ๒๔ กันยายน ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย นายจิรชาติ วงศ์ทอง ผู้อำนวยการฝ่ายตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งปรีกษาและเจ้าหน้าที่จากสำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้แจ้งผลการประเมินและให้คำปรึกษาแก่กองทุนเงินให้กู้ยืมเพื่อการศึกษา ในการจัดทำแผนการปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อยกระดับขีดความสามารถในการป้องกันภัยไซเบอร์ขององค์กรให้มีประสิทธิภาพสูงสุด การประชุมครั้งนี้มี นางสาวนันทวัน วงศ์ขจรกิตติ รองผู้จัดการกองทุนฯ นายอาสิน ไชยกุล ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ และเจ้าหน้าที่ด้านเทคโนโลยีที่เกี่ยวข้องร่วมรับฟังผลการประเมินและแนวทางในการปรับปรุง ทั้งนี้เพื่อให้หน่วยงานสามารถดำเนินการยกระดับความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพยิ่งขึ้น

๓.๙.๒.๒ บริษัท โกโกลูก (ประเทศไทย) จำกัด

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ โดย ลธ.กมช. ได้จัดพิธีลงนามบันทึกความเข้าใจความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับ บริษัท โกโกลูก (ประเทศไทย) จำกัด โดย Mr. Jeff Kuo ประธานเจ้าหน้าที่บริหาร เมื่อวันที่ ๑๗ มกราคม ๒๕๖๗ ณ ห้องประชุม Confidential ชั้น ๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นที่เรียบร้อยแล้ว และได้ดำเนินงานร่วมกัน ดังนี้

๑. วันอังคารที่ ๙ มกราคม ๒๕๖๗ สำนักงาน

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ นำโดย พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหารือร่วมกับ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และบริษัท Gogolook ประเทศไทย ผู้พัฒนาแอป Whoscall เพื่อหารือแนวทางป้องกันการฉ้อโกงของมิจฉาชีพและการพัฒนาเทคโนโลยีเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคลและความเป็นส่วนตัวของประชาชนชาวไทย พร้อมตอบข้อซักถามเกี่ยวกับประเด็นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของ app ดังกล่าว โดยได้เน้นย้ำการสร้างแผนป้องกันที่ครอบคลุมและมีประสิทธิภาพ เพื่อพัฒนาสังคมไทยในยุคดิจิทัลให้มีความปลอดภัยและน่าเชื่อถือยิ่งขึ้น

๒. บริษัท Gogolook ผู้พัฒนา Whoscall ร่วมหารือ

ความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อผลักดันและสนับสนุนการป้องกันภัยคนไทยไม่ให้ถูกล่อลวง ด้วยการสร้างระบบข้อมูล ยืนยันการรับรองเบอร์โทรสำหรับหน่วยงานภาครัฐ และระบบข้อมูล Blacklist สำหรับเหล่ามิจฉาชีพ และการทำงานร่วมกันของทั้ง ๒ หน่วยงานในอนาคต

๓.๙.๒.๓ กรมการขนส่งทางบก (ขบ.)

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ โดย ลธ.กมช. ได้จัดพิธีลงนามบันทึกความเข้าใจความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับ กรมการขนส่งทางบก (ขบ.) โดย นายจิรุตม์ วิศาลจิตร ตำแหน่ง อธิบดีกรมการขนส่งทางบก เมื่อวันที่ ๓๑ มกราคม ๒๕๖๗ ณ ศูนย์ประชุมแห่งชาติสิริกิติ์ เป็นที่เรียบร้อยแล้ว และในวันศุกร์ที่ ๒ สิงหาคม ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย เรืออากาศเอก นพรัตน์ สุจินดา ผู้อำนวยการฝ่ายทดสอบเจาะระบบและประเมินความพร้อม สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ร่วมเป็นวิทยากรบรรยายเรื่อง "ภัยไซเบอร์ ด้านมืดในโลกดิจิทัล" เพื่อส่งเสริมให้บุคลากรมีความตระหนักรู้เกี่ยวกับการใช้สื่อออนไลน์ และการรักษาความมั่นคงปลอดภัยไซเบอร์ ณ ห้องประชุมอาคาร ๖ กรมการขนส่งทางบก

๓.๙.๒.๔ กองทัพอากาศ

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ โดย ลธ.กมช. ได้จัดพิธีลงนามบันทึกความเข้าใจความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับ กองทัพอากาศ (ทอ.) โดย พลอากาศเอก พันธุ์ภักดี พัฒนกุล ตำแหน่ง ผู้บัญชาการทหารอากาศ เมื่อวันที่ ๙ กุมภาพันธ์ ๒๕๖๗ ณ ห้องรับรองพิเศษ ๑ กองบัญชาการกองทัพอากาศ เป็นที่เรียบร้อยแล้ว และได้ดำเนินงานร่วมกัน ดังนี้

๑. เมื่อวันอังคารที่ ๒๐ กุมภาพันธ์ ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ นำโดย พลตรี ธีรวุฒิ วิทยากรณ์ รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พร้อมคณะ ให้การต้อนรับ พลอากาศตรี สมพร ร่มพยอม ผู้อำนวยการศูนย์ไซเบอร์กองทัพอากาศ ผู้บังคับบัญชา คณาจารย์ และนายทหารนักเรียนจากศูนย์ไซเบอร์กองทัพอากาศ ซึ่งการศึกษาดูงานในครั้งนี้ ได้มีการบรรยายแนะนำหน่วยงาน เพื่อให้ทราบภารกิจ ผลงานที่สำคัญที่ผ่านมาของ สกมช. และรูปแบบภัยคุกคามทางไซเบอร์ที่พบในปัจจุบัน ตลอดจนการปฏิบัติการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) นอกจากนี้ ยังเป็นการต่อยอดความร่วมมือระหว่าง สกมช. และ ศูนย์ไซเบอร์กองทัพอากาศ ในการสนับสนุนการเสริมสร้างทักษะความรู้กำลังคนด้านไซเบอร์ เพื่อร่วมกันสร้างความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศต่อไป

๒. วันอังคารที่ ๒๙ พฤษภาคม ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย พันตำรวจเอก ณ์ทกฤษ พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ ในขณะนั้นเป็นวิทยากรบรรยายพิเศษ ให้กับนักเรียนเสนาธิการทหารอากาศ ในหัวข้อ “การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” โดยมีวัตถุประสงค์ เพื่อสร้างความตระหนักรู้ และวิธีป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยได้แลกเปลี่ยนประสบการณ์และเน้นย้ำให้ตระหนักถึงผลกระทบของภัยคุกคามทางไซเบอร์ที่ปัจจุบันทวีความรุนแรงมากขึ้น ณ โรงเรียนเสนาธิการทหารอากาศ กรมยุทธศึกษาทหารอากาศ

๓.๙.๒.๕ บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด
ข้อรายงาน

Government Security Program (GSP) เป็นโครงการระดับโลกของไมโครซอฟท์ที่เริ่มต้นในปี ๒๕๔๖ มีเป้าหมายเพื่อเสริมสร้างความสามารถในการปกป้องบุคลากร ข้อมูล และโครงสร้างพื้นฐานจากภัยคุกคามไซเบอร์ GSP เป็นกลไกสำคัญในการสร้างความร่วมมือระหว่างไมโครซอฟท์และรัฐบาล โดยดำเนินการภายใต้กรอบกฎหมายและการดำเนินงานที่เป็นเอกภาพซึ่งช่วยให้สามารถตัดสินใจเกี่ยวกับเทคโนโลยีได้อย่างมีข้อมูล ปัจจุบันโครงการนี้ครอบคลุมการร่วมมือกับกว่า ๔๐ ประเทศและองค์กรระหว่างประเทศกว่า ๑๐๐ แห่ง ภายใต้ข้อตกลงนี้ ไมโครซอฟท์และ NCSA ได้ร่วมกันแลกเปลี่ยนข้อมูลและความรู้เกี่ยวกับเรื่องต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงรายละเอียดทางเทคนิคเกี่ยวกับภัยคุกคาม ความเปราะบาง ความผิดปกติ ข้อมูลเกี่ยวกับมัลแวร์ และปัญหาด้านความมั่นคงปลอดภัยที่สำคัญที่เกี่ยวข้องกับผลิตภัณฑ์และบริการของไมโครซอฟท์ ในอนาคต ทั้งสองฝ่ายอาจพิจารณาขยายความร่วมมือเพื่อรวมถึงการเข้าถึงเอกสารทางเทคนิคหรือซอร์สโค้ดของผลิตภัณฑ์และบริการของไมโครซอฟท์ ซึ่งอาจรวมถึงการทบทวนและวิเคราะห์เอกสารทางเทคนิคและซอร์สโค้ดที่หนึ่งในห้าศูนย์ความโปร่งใสของไมโครซอฟท์ที่ตั้งอยู่ทั่วโลกในสหรัฐอเมริกา ไอร์แลนด์ สิงคโปร์ บราซิล และจีน

นอกจากนี้ ไมโครซอฟท์และ NCSA จะร่วมกันส่งเสริมและขับเคลื่อนความรู้ ความเข้าใจ และทักษะในการกำกับดูแล AI อย่างปลอดภัยและรับผิดชอบ ซึ่งจะดำเนินการผ่านโปรแกรมการฝึกอบรมที่มุ่งเน้นไปที่ Copilot for Security และการใช้ AI เพื่อสนับสนุนความพยายามด้านความมั่นคงปลอดภัยไซเบอร์ โปรแกรมเหล่านี้จะมีเป้าหมายที่หน่วยงานรัฐบาลและบุคลากรที่รับผิดชอบในการจัดการโครงสร้างพื้นฐานข้อมูลที่สำคัญ (CII)

ทั้งนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้จัดพิธีลงนามข้อตกลงโครงการ Government Security Program กับ บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด ซึ่งผู้แทนทั้ง ๒ ฝ่ายได้ดำเนินการให้ผู้บริหารลงนาม โดย Mr. Anthony Rice ตำแหน่ง Principal Security PM Manager เป็นผู้ลงนามฝ่ายบริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด ลงนามเมื่อวันที่ ๑๐ เมษายน ๒๕๖๗ และพลอากาศตรี อมร ชมเชย เป็นผู้ลงนามฝ่าย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ลงนามเมื่อวันที่ ๑๑ เมษายน ๒๕๖๗ ณ และได้มีการดำเนินงานร่วมกันเมื่อวันที่ ๑ พฤษภาคม ๒๕๖๗ พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เข้าร่วมงาน Microsoft Build AI Day Event & Exclusive CEO Connection โดยมี นายเศรษฐา ทวีสิน นายกรัฐมนตรี และนายประเสริฐ จันทรรวงทอง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เข้าร่วม ณ ศูนย์การประชุมแห่งชาติสิริกิติ์ โดย ไมโครซอฟท์ (Microsoft) ประกาศแผนงานด้านโครงสร้างพื้นฐาน ครอบคลุมถึงการการจัดตั้ง Data and AI Center ระดับภูมิภาคแห่งใหม่ในประเทศไทย เพื่อขยายการให้บริการคลาวด์ให้กว้างขวางและทั่วถึงยิ่งขึ้น รวมทั้งการพัฒนาทักษะด้าน AI ให้กับบุคลากรคนไทย กว่า ๑๐๐,๐๐๐ คน พร้อมกับสนับสนุนชุมชนนักพัฒนาในประเทศไทย และนำไปสู่การสร้างสภาพแวดล้อมของการเป็น Digital Economy Hub หรือ ฮับเศรษฐกิจดิจิทัล ตามวิสัยทัศน์ “IGNITE THAILAND” ของรัฐบาล ซึ่งที่ผ่านมา สกมช. ร่วมเป็นส่วนหนึ่งในการส่งเสริมนโยบาย Cloud Security First และมุ่งขับเคลื่อนมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ เพื่อให้เกิดโครงสร้างพื้นฐานที่ปลอดภัย และจะดำเนินการประสานงานร่วมกับ Microsoft เพื่อประโยชน์ของประเทศต่อไป

๓.๙.๒.๖ สมาคมสันนิบาตเทศบาลแห่งประเทศไทย

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย สท.กมช. ได้จัดพิธีลงนามบันทึกความเข้าใจความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับ สมาคมสันนิบาตเทศบาลแห่งประเทศไทย (ส.ท.ท.) โดย นายสมชาย รังสีวัฒนศักดิ์ ตำแหน่งนายกสมาคมสันนิบาตเทศบาลแห่งประเทศไทย เมื่อวันที่ ๑๐ มิถุนายน ๒๕๖๗ ณ ห้องประชุม Confidential ชั้น ๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นที่เรียบร้อยแล้ว และได้มีการดำเนินงานร่วมกันเมื่อวันเสาร์ที่ ๖ มกราคม ๒๕๖๗ พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ บรรยายในหัวข้อ “ภัยไซเบอร์ต่อชุมชนและประชาชน” ในการประชุมและการสัมมนาวิชาการ สมาคมสันนิบาตเทศบาลแห่งประเทศไทย ซึ่งเป็นการจัดประชุมสัมมนาวิชาการ แลกเปลี่ยนประสบการณ์และขยายผลความคิดสร้างสรรค์ผลงานของแต่ละท้องถิ่น เพื่อพัฒนาไปสู่การเป็นท้องถิ่นดิจิทัล รวมถึงสามารถนำไปพัฒนาเมืองและคุณภาพชีวิตประชาชนให้ดีขึ้นในทุกมิติ ระหว่างวันที่ ๔ - ๖ มกราคม ๒๕๖๗ ณ ศูนย์ประชุมและแสดงสินค้านานาชาติเฉลิมพระเกียรติ ๗ รอบพระชนมพรรษา จังหวัดเชียงใหม่

๓.๙.๒.๗ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ โดย ลธ.กมช. ได้จัดพิธีลงนามบันทึกความเข้าใจความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) โดย นางไอรดา เหลืองวิไล ตำแหน่ง รองผู้อำนวยการ รักษาการแทนผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เมื่อวันที่ ๑๐ มิถุนายน ๒๕๖๗ ณ ห้องประชุม Confidential ชั้น ๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นที่เรียบร้อยแล้ว และได้มีการดำเนินงาน ดังนี้

๑. สกมช. กับ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ร่วมมือกันจัดกิจกรรมซ้อมแผนด้านความมั่นคงปลอดภัยทางไซเบอร์ Sectoral CERT ด้านพลังงาน กระทรวงพลังงาน ประจำปี พ.ศ. ๒๕๖๗ Energy Sector Cyber Exercise ๒๐๒๔ วันพุธที่ ๔ กันยายน ๒๕๖๗ นำโดย นางสาวสายชล แซ่ลี ผู้อำนวยการสำนักประสานงาน ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และ เรือโท อธิพล หนองหว่า พร้อมเจ้าหน้าที่จาก ThaiCERT สกมช. ร่วมเป็นวิทยากร ทั้งนี้ สกมช. ได้จำลองกิจกรรม Cyber War Game Simulation ซักซ้อมการเผชิญเหตุภัยคุกคามทางไซเบอร์ โดยได้รับการสนับสนุนระบบจากบริษัท Dnative Co.,Ltd. ซึ่งมีผู้เข้าร่วมกว่า ๖๐ คน โดยจัดกิจกรรมในครั้งนี้มีวัตถุประสงค์เพื่อให้มีความเข้าใจและทราบถึงปัจจัยความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่ต้องคำนึงถึง รวมทั้งแนวทางการบริหารความเสี่ยง การตอบสนอง รับมือ และการตัดสินใจในสถานการณ์เมื่อเกิดภัยคุกคามทางไซเบอร์ เพื่อให้เกิด Cyber Resiliency และลดผลกระทบต่อการดำเนินงานได้ ณ ศูนย์เอนเนอร์ยีคอมเพล็กซ์ อาคารบี กระทรวงพลังงาน

๒. เมื่อวันพฤหัสบดีที่ ๘ สิงหาคม ๒๕๖๗ นางสาวสายชล แซ่ลี และเจ้าหน้าที่จาก สกมช. ร่วมเป็นวิทยากรจัดกิจกรรม Cyber War Game Simulation ผ่านการเผชิญเหตุภัยคุกคามทางไซเบอร์ โดยได้รับการสนับสนุนระบบจากบริษัท Dnative Co.,Ltd. ซึ่งมีผู้เข้าร่วมกว่า ๓๐ คน โดยจัดกิจกรรมเพื่อให้มีความเข้าใจและทราบถึงปัจจัยความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่ต้องคำนึงถึง รวมทั้งแนวทางการบริหารความเสี่ยง การตอบสนอง รับมือและการตัดสินใจในสถานการณ์เมื่อเกิดภัยคุกคามทางไซเบอร์ เพื่อให้เกิด Cyber Resiliency และลดผลกระทบต่อการดำเนินงานได้ ณ อาคารดิออปฟิเคส แอท เซ็นทรัลเวิลด์ กรุงเทพมหานคร

๓.๙.๒.๘ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข

ข้อรายงาน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ โดย ลธ.กมช. ได้จัดพิธีลงนามบันทึกความเข้าใจความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับ กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข (สบส.) โดย นายสุระ วิเศษศักดิ์ ตำแหน่ง อธิบดีกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข เมื่อวันที่ ๒๑ สิงหาคม ๒๕๖๗ ณ ห้องประชุมสุขศึกษา อาคารกรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข เป็นที่เรียบร้อยแล้ว และได้มีการดำเนินงาน ดังนี้

๑. เมื่อวันพฤหัสบดีที่ ๒ พฤศจิกายน พ.ศ. ๒๕๖๖ พลอากาศตรี อมร ชมเชย เลขานุการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พร้อมด้วยคณะผู้บริหาร สกมช. เข้าพบ อธิบดีกรมสนับสนุนบริการสุขภาพ เพื่อหารือแนวทางการสร้างเครือข่ายร่วม อสม. เพื่อพัฒนาอาสาสมัครสาธารณสุขประจำหมู่บ้าน (อสม.) ให้มีทักษะในการใช้เทคโนโลยีดิจิทัล (Digital

Literacy) ได้อย่างปลอดภัย ป้องกันการถูกหลอกลวงจากมิจฉาชีพ และสามารถถ่ายทอดให้กับประชาชนได้ ด้วย โดยใช้ช่องทางเข้าถึง อสม. ด้วยการใช้แอปพลิเคชันให้ความรู้และคำแนะนำสำหรับอาสาสมัครประจำหมู่บ้าน ผ่าน “แอปพลิเคชัน สมาร์ท อสม.” ซึ่งจะเป็นตัวช่วยส่งเสริม ทักษะในการตระหนักรู้วิธีป้องกันภัยไซเบอร์ให้ถึง อสม. ที่มีอยู่ประมาณ ๑.๗ ล้านคนทั่วประเทศ ให้เกิดภูมิคุ้มกันด้านไซเบอร์เพื่อให้ใช้ได้ดิจิทัลได้อย่างปลอดภัย

๒. เมื่อวันศุกร์ที่ ๒ กุมภาพันธ์ ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย พันตำรวจเอก ณ์ทกฤษ พรหมจันทร์ ผู้อำนวยการสำนักปฏิบัติการ และเรือโท ธีรพล หนองหว้า ผู้อำนวยการฝ่ายตอบสนองและรับมือภัยคุกคามทางไซเบอร์ สำนักปฏิบัติการ ในขณะนั้น ร่วมเป็นวิทยากรอบรมเชิงปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยและการป้องกันภัยคุกคามไซเบอร์ จัดขึ้นโดย กรมสนับสนุนบริการสุขภาพ มีวัตถุประสงค์เพื่อสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์และลดความเสี่ยงจากภัยคุกคามไซเบอร์ แก่บุคลากรในสังกัดกรมสนับสนุนบริการสุขภาพ ณ ห้องประชุมสุขศึกษาชั้น ๙ อาคารกรมสนับสนุนบริการสุขภาพ

๓.๙.๒.๙ บริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด

ข้อรายงาน

สำนักงานคณะกรรมการการักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ร่วมกับบริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด จัดการแข่งขัน Thailand Cyber Top Talent รอบชิงชนะเลิศ เมื่อวันที่ ๑๒ ตุลาคม ๒๕๖๗ โดยมีทีมเข้าร่วมแข่งขันจำนวน ๓๐ ทีม ผู้เข้าแข่งขันทั้งสิ้น จำนวน ๙๐ คน ซึ่งเป็นการแข่งขัน CTF jeopardy รูปแบบ Attack the virtual World ชิงเงินรางวัลมูลค่ารวม ๕๒๑,๐๐๐ บาท และได้ทีมระดับอุดมศึกษา เป็นตัวแทนประเทศไทยเข้าร่วมแข่งขัน Cyber SEA Game ๒๐๒๔ เมื่อวันที่ ๒๔ - ๒๕ ตุลาคม ๒๕๖๗ มีผู้เข้าร่วมแข่งขันทั้งหมด จำนวน ๘๔๖ ทีม แบ่งออกเป็น ๓ ระดับ ได้แก่ ระดับมัธยมศึกษา ระดับอุดมศึกษา และระดับประชาชนทั่วไป รวมทั้ง ๓ ระดับ จำนวน ๒,๔๐๘ คน ทั่วทุกภูมิภาคประเทศไทย และได้ทีมในแต่ละระดับเข้าร่วมแข่งขันรอบชิงชนะเลิศ จำนวนรวม ๓๐ ทีม

ฝ่ายเลขานุการขอเสนอต่อที่ประชุมรับทราบผลการดำเนินงาน เสริมสร้างความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จากการลงนามบันทึกความร่วมมือระหว่าง สำนักงานคณะกรรมการการักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ หน่วยงานต่าง ๆ ดังนี้

๑. กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.)
๒. บริษัท โกลบอล (ประเทศไทย) จำกัด
๓. กรมการขนส่งทางบก (ขบ.)
๔. กองทัพอากาศ (ทอ.)
๕. บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด
๖. สมาคมสันนิบาตเทศบาลแห่งประเทศไทย (ส.ท.ท.)
๗. สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
๘. กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข (สบส.)
๙. บริษัท หัวเว่ย เทคโนโลยี (ประเทศไทย) จำกัด

มติที่ประชุม รับทราบผลการดำเนินงานเสริมสร้างความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จากการลงนามบันทึกความร่วมมือระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ หน่วยงานต่าง ๆ

ระเบียบวาระที่ ๔ เรื่องเพื่อพิจารณา

๔.๑ สรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ประจำปี ๒๕๖๗

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมขอให้พลตรี ธีรวุฒิ วิทยาภรณ์ รองเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ฐานอำนาจ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙ (๑๒) บัญญัติว่า “คณะกรรมการมีหน้าที่และอำนาจ จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ”

ความเป็นมา

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ข้อรายงาน

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการเฝ้าระวัง ตรวจสอบประเมินความเสี่ยง สนับสนุนและให้คำแนะนำเพื่อในการแก้ปัญหาภัยคุกคามทางไซเบอร์ให้กับหน่วยงานต่าง ๆ ในห้วง ตุลาคม ๒๕๖๖ – กันยายน ๒๕๖๗ มีผลการดำเนินการ ดังนี้

สถิติการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์

(๑) แยกประเภทการโจมตีทางไซเบอร์

ประเภทภัยคุกคามทางไซเบอร์	จำนวน (เหตุการณ์)	สัดส่วนร้อยละ (%)
Hacked Website - Defacement (๒๙๒) ร้อยละ ๑๖ - Gambling (๒๕๘) ร้อยละ ๑๔ - Malware (๒๐) ร้อยละ ๑ - Phishing (๒๑) ร้อยละ ๑ - Hacked Website (๔) ร้อยละ ๑	๕๙๕	๓๐
Fake Website	๒๔๕	๑๓
Privileged Account Compromise	๑๘๑	๑๐

ประเภทภัยคุกคามทางไซเบอร์	จำนวน (เหตุการณ์)	สัดส่วนร้อยละ (%)
จุดอ่อนช่องโหว่ (Vulnerability)	๑๘๑	๑๐
Finance Scam - หลอกลวงการเงิน Online	๑๖๓	๙
ข้อมูลรั่วไหล (Data Breach)	๑๒๙	๗
DDoS	๕๘	๓
Security Misconfiguration	๕๔	๓
Data Leak	๔๒	๒
Credential Leak	๓๕	๒
Ransomware	๓๔	๒
Unauthorised modification of information	๓๒	๒
Account Compromise	๒๑	๑
อื่น ๆ	๕๗	๖
รวมทั้งสิ้น	๑,๘๒๗	๑๐๐

(๒) แยกประเภทหน่วยงานที่ได้รับผลกระทบ แยกตามภารกิจหรือบริการ

ประเภทหน่วยงานที่ได้รับการสนับสนุน แบ่งตามภารกิจหรือบริการ	จำนวน (เหตุการณ์)	สัดส่วนร้อยละ (%)
๑. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๑.๑ ด้านความมั่นคง ๑.๒ ด้านบริการภาครัฐ ๑.๓ ด้านการเงินการธนาคาร ๑.๔ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ๑.๕ ด้านขนส่งและโลจิสติกส์ ๑.๖ ด้านพลังงานและสาธารณูปโภค ๑.๗ ด้านสาธารณสุข	๒๙๘ ๔๓ ๓ ๑๓๓ ๓๐ ๔ ๘๓ ๒	๑๖%
๒. หน่วยงานควบคุมหรือกำกับดูแล ๒.๑ ด้านความมั่นคง ๒.๒ ด้านบริการภาครัฐ ๒.๓ ด้านการเงินการธนาคาร ๒.๔ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ๒.๕ ด้านขนส่งและโลจิสติกส์ ๒.๖ ด้านพลังงานและสาธารณูปโภค ๒.๗ ด้านสาธารณสุข	๕๑ ๗ ๒๒ ๑ ๘ ๑ ๑๐ ๒	๔%
๓. หน่วยงานของรัฐ ๓.๑ ด้านความมั่นคง ๓.๒ ด้านบริการภาครัฐ ๓.๓ ด้านการเงินการธนาคาร	๑,๐๓๓ ๓๗ ๗ ๑	๕๖%

ประเภทหน่วยงานที่ได้รับการสนับสนุน แบ่งตามภารกิจหรือบริการ	จำนวน (เหตุการณ์)	สัดส่วนร้อยละ (%)
๓.๔ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม	๙	
๓.๕ ด้านขนส่งและโลจิสติกส์	๑๒	
๓.๖ ด้านพลังงานและสาธารณูปโภค	๔	
๓.๗ ด้านสาธารณสุข	๖๐	
๓.๘ ด้านการศึกษา	๕๑๙	
๓.๙ หน่วยงานของรัฐ ด้านอื่น ๆ	๓๘๑	
๓.๑๐ ด้านอื่น ๆ	๓	
๔. หน่วยงานเอกชน	๔๔๕	๒๔%

การปฏิบัติตามมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์
ห้วง ตุลาคม ๒๕๖๖ – กันยายน ๒๕๖๗

(๑) การปฏิบัติตามมาตรการเชิงรุก

ก. การแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน ๙๐ รายงาน
 ข. การเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์และข่าวสารที่เป็นประโยชน์
 ต่อสาธารณะ จำนวน ๔๔๙ รายงาน
 ค. การทดสอบความปลอดภัยของระบบเครื่องแม่ข่ายและเว็บไซต์ จำนวน
 ๑๑๑ หน่วยงาน

(๒) การปฏิบัติตามมาตรการเชิงรับ

ก. การแจ้งเตือนเหตุการณ์และให้คำแนะนำในการแก้ไขปัญหา จำนวน
 ๑,๘๒๗ หน่วยงาน

ข. การตอบสนองและรับมือภัยคุกคามทางไซเบอร์ จำนวน ๓๖ หน่วยงาน

(๓) การบริหารจัดการคุณภาพ

การสร้างความรู้ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน ๗๓ ครั้ง
 มีผู้เข้าร่วมทั้งสิ้น ๙,๘๕๔ คน

นายเฉลิมศักดิ์ เลิศวงศ์เสถียร ผู้แทนปลัดกระทรวงการคลัง อย่างแรกต้อง
 ขอขอบคุณทีม ThaiCERT คือกระทรวงการคลังเคยได้รับสนับสนุนการช่วยเหลือเป็นอย่างดี และคิดว่า
 หน่วยงานรัฐหลายหลายแห่งก็ได้รับการแจ้งเตือนและข้อเสนอแนะจากทาง ThaiCERT เป็นอย่างดี ข้อที่สอง
 ผมมองว่า SectoralCERT เป็นเรื่องสำคัญเนื่องจากว่า สกมช. เป็นเหมือนหน่วยงานการที่ช่วยเหลือหน่วยงาน
 ราชการทั้งหมดบางครั้งเหมือนที่เราจะสร้าง SectoralCERT ที่เข้มแข็งออกมาได้มันจะช่วยให้กลุ่มนั้น ๆ
 สามารถที่จะมีการแจ้งเตือนและการดูแลตัวเองได้อย่างรวดเร็วและทันทั่วทั้ง สกมช. คงค่อนข้างหนักและ
 เหนื่อยตามการส่งการแจ้งเตือนและต้องช่วยติดตามข้อมูล ผมเข้าใจว่า SectoralCERT ในปัจจุบันมีการแจ้ง
 และตั้งขึ้นมาเพียงแต่ว่ามันมีช่องว่างที่เกิดขึ้นในปัจจุบันระหว่างหน่วยงานกับที่นำไปกลับหน่วยการ งานที่
 เสนอ ขึ้นตั้งเรียบร้อยแต่ว่าการดำเนินงานยังไม่ดำเนินการเต็มรูปแบบในเรื่องของการตั้ง SectoralCERT
 น่าจะผลักดันการให้ข้อมูลของ การให้ความรู้ติดตามเรื่องของความก้าวหน้าของ SectoralCERT จะทำให้การ
 กระจายหรือการแจ้งเตือนมีช่องว่างลดลง ประเด็นที่สองเรื่องของเครื่องมือที่ใช้ติดตามตัว ของ สกมช. หรือ
 หน่วยงานอื่น ๆ ได้รับข้อมูลข่าวสารจะวิ่งไปหาเครื่องมือที่มีลักษณะลักษณะคล้าย ๆ กัน พอได้รับข้อมูลจาก

ThaiCERT ทางเราก็ก็นำไปศึกษาเหมือนกันอย่างเช่น เรื่องของความคุ้มค่าเพราะว่าเครื่องมือหลายกลุ่มก็จะราคาให้เพื่อให้หน่วยงานมีการลงทุนอย่างมีประสิทธิภาพ ซึ่งใน สกมช. จะมีต้นแบบที่ดีสำหรับการทดลองและมีการใช้เครื่องมือหลายตัว

พลตำรวจตรี ชูศักดิ์ ขนาดนิต ผู้แทนผู้บัญชาการตำรวจแห่งชาติ จากที่รายงาน เราจะเห็นว่าปัจจุบันคนร้ายใช้แพลตฟอร์มต่าง ๆ ของต่างประเทศทำผิดในประเทศไทย แต่เวลาขอความร่วมมือกับ Meta หรือ LINE ช่วยปิดก่อนที่จะล่อลวงหรือใช้รูปคนสำคัญมาล่อลวงปรากฏว่าความร่วมมือน้อยมาก LINE ให้ความร่วมมือปิดไม่เกิน ๑๐% Meta ให้ความร่วมมือปิดไม่เกิน ๔๐% ที่ทางบริษัทจะปิดให้โดยทำหนังสือส่งคำร้องไปที่ทางบริษัทแต่ความร่วมมือจริง ๆ ซึ่งกฎหมายก็ไม่สามารถบังคับได้เพราะเค้าจะอ้างว่า Sever อยู่ต่างประเทศเลยอยากจะให้คณะกรรมการช่วยกันคิดว่าควรจะมีกฎหมายอะไรควบคุมพวกแพลตฟอร์มที่มามีในในประเทศไทยเพราะเขาได้ค่าโฆษณาไปจากประเทศไทยค่อนข้างเยอะแต่ไม่ค่อยปฏิบัติตามกฎหมายไทย

นายไพบูลย์ อมรปัญญาเกียรติ กรรมการผู้ทรงคุณวุฒิฯ จริง ๆ เรามีกฎหมายในเรื่องของดิจิทัลแพลตฟอร์มของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์หรือ สทอ. ในขณะนี้อยู่ในระหว่างการจัดตั้งก็คิดว่าน่าจะใช้ได้ ล่าสุดอย่างกรณีของ สคส. จะมีปัญหาในเรื่องของข้อมูลรั่วไหลมี Scammer และมีกรณีละเมิดสิทธิเด็กและยาเสพติดค่อนข้างเยอะ ล่าสุด สคส. ได้เชิญ FacebookThailand ซึ่งเขาจะมีช่องทาง fast track ให้ในกรณีที่มีข้อมูลส่วนบุคคลจะลบทันทีซึ่งจะรวมถึงกรณีของ Instagram ตามนโยบายของประธานเรามีนโยบายที่จะเรียก LINE YouTube Google มาด้วยเช่นกัน ส่วนในเรื่องการจัดเก็บภาษีช่วงของรัฐบาลที่แล้วเราได้เก็บภาษี Facebook และ Google แล้วการตีความล่าสุด เมื่อสองปีที่แล้วของสรรพากรสมัยที่ท่านเอกนิติฯ เป็นอธิบดีกรมสรรพากร ได้ตีความว่าถือเป็นการได้ประโยชน์การให้บริการของประเทศไทยเดิมจากการจ่ายภาษีแค่หลักล้านล่าสุดกรมสรรพากรเก็บเป็นเงินจำนวน ๑๐๐ ล้านบาทถ้าท่านประธานหรือรัฐบาลจะเก็บต่อถือเป็นเรื่องที่ดีและเงินเป็นจำนวนค่อนข้างสูง

พลตำรวจตรี ชูศักดิ์ ขนาดนิต ผู้แทนผู้บัญชาการตำรวจแห่งชาติ ขอบคุณมากครับเดี๋ยวผมจะตอบประธานอีกทีเพราะผมมีเว็บไซต์สำหรับรับเรื่องร้องเรียนที่เกี่ยวข้องกับการปลอม Facebook จำนวนค่อนข้างเยอะ

นายรัชกรณ นภาพรพิพัฒน์ ผู้แทนสภาความมั่นคงแห่งชาติ ในเอกสารมีการเขียนกลุ่ม RipperSec มีแนวโน้มว่าสูงขึ้นซึ่งในเอกสารระบุว่า เป็น hacker ที่มีชื่อเสียง และมีวัตถุประสงค์การโจมตีการเมืองเป็นหลัก ตามเอกสารที่ ๓๖

นายปริญญา หอมอนเณ กรรมการผู้ทรงคุณวุฒิฯ ขอบธิบายเพิ่มเติม RipperSec เขาเป็นกลุ่ม ๓ จังหวัด ชายแดนภาคใต้กลุ่มผู้ก่อการร้าย ถ้าเกิดเค้าจะถล่มธนาคารของไทยเค้าบอกว่า ๙ โมงเช้าของวันพรุ่งนี้ เค้าจะยิงมาพอถึงเวลาที่ล่มจริงเลยเวลา ๙ โมงจะเข้าไม่ได้เลย แต่ในขณะนี้ทุกแบงค์ รวมถึง TB-CERT ได้มีโซลูชัน Data Scrubbing ต้องจัดตัวยิงพวกนี้ทิ้งออกไปแต่การทำแบบนี้มันต้องใช้เงินแต่ถ้าเป็นหน่วยงานรัฐ แต่ถ้ายิงมาหน่วยงานรัฐจะลำบาก เพราะว่าอุปกรณ์ป้องกัน Anti-DDoS นี้จะไม่ได้อยู่ใน Dark web แล้วจะมีน้อยแต่จะเพิ่มขึ้นใน Telegram ที่เจ้าของเครื่องโดนจับไปในประเทศรัสเซียสามารถเข้าไปใน Telegram ของตำรวจน่าจะได้อะไรเยอะและถ้าเกิดจะก่อเหตุกับหน่วยงานก็จะประกาศแต่ปัญหามันมีอยู่ว่ากลุ่มนี้จะแจก tool ให้กับประชาชนและบุคคลทั่วไป บางครั้งเด็ก ๆ ได้มาก็เอามายิงเลยต้องติดตามใน Telegram ทีมที่ต่อผมมีข้อมูลสามารถให้ได้

พลอากาศตรี อมร ชมเชย ชี้แจงเพิ่มเติม RipperSec ทำเพื่อเงินเป็นกลุ่ม Ransomware ซึ่งปัจจุบันนี้นอกจากการโจมตี หน่วยงานรัฐมีแนวโน้มลดลงแต่ไปโจมตีภาคเอกชน เพราะภาคเอกชนมีโอกาสที่จะจ่ายเงินค่าไถ่มากกว่าหน่วยงานรัฐแต่ตอนนี้จะเสียหายไปพักหนึ่งเพราะโดนทะเลาะถูกเอาผิดออกมา แต่ตอนนี้กำลังเริ่มใหม่กลุ่มนี้นอกจากการโจมตีใช้เครื่องมือ และกลุ่มของตัวเองจะร่วมมือกับคนภายใน หน่วยงานด้วยเพื่อให้คนใน ให้ User และ Password มาโจมตีสำเร็จและแชร์ค่าไถ่ และเป็นกลุ่มที่มี Active ภายในประเทศไทยเลยเป็นส่วนที่เราต้องดำเนินการติดตามให้ทราบถึงแนวโน้ม Indicator การโจมตีในลักษณะ ต่าง ๆ ให้เราได้เตรียมรับมือต่อไป

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี เรื่องนี้เป็นเรื่องเพื่อพิจารณาขอเพิ่มเติมที่ หลาย ๆ ท่านให้ความคิดเห็นเรื่องของแพลตฟอร์มต่างประเทศท่านนายกได้สั่งการในการประชุม ครม. ในเรื่องของการกำกับดูแลในกระทรวงดิจิทัลเป็นส่วนหนึ่งในการทำงานร่วมกับหลายภาคส่วนในหลายประเด็น อย่างที่ได้ยกมาเช่นคุณภาพสินค้าการจัดตั้ง เป็นต้นคาดว่าจะประชุมภายในสัปดาห์หน้าสำหรับเรื่องนี้ เรื่องที่ สองการขายข้อมูลใน Dark web ขอยกตัวอย่าง จากการรายงานของท่านอมรฯ เวลาที่รายงานรัฐมนตรีจะมีการ ขายข้อมูลจาก Dark web ตลอดในเรื่องนี้เราสามารถดำเนินคดีกับผู้ขายที่อยู่ต่างประเทศได้หรือไม่ รวมถึงผู้ ให้บริการเจ้าของแพลตฟอร์มเช่น Facebook หรือ TikTok ไม่แน่ว่าเราจะดำเนินการคดีกับบริษัทได้ไหม

นายไพบูลย์ อมรวิญญูเกียรติ กรรมการผู้ทรงคุณวุฒิฯ เพิ่มเติมข้อมูลในส่วนของ Facebook ถือว่าเค้าเป็นผู้ถือข้อมูลส่วนบุคคล และเป็นผู้ประมวลผลในประเด็นนี้ได้หยิบยกมาพูดถึงการขาย ข้อมูลบน Dark web ซึ่งทางบริษัทเขาก็ยอมรับ ในขณะนี้ที่ EU เริ่มดำเนินการปรับบริษัทแล้ว อย่างที่ท่าน ประธานพูดเราเตือนไปหนึ่งครั้งแล้ว แต่ก็ยังมีการขายอยู่เดี๋ยวทางเราจะปรับเหมือนกับทาง EU ซึ่งจะเชิญให้ทาง บริษัทมาพบกับท่านรัฐมนตรี โดยสามารถเปิดช่องทางพิเศษให้กับเราเพราะว่าโดยหลักกฎหมาย แต่ผิดกฎหมาย PDPA ท่านสามารถสั่งปรับได้เลย ถ้ากรณีธรรมดาสั่งปรับจำนวนเงิน สามล้านบาทต่อหนึ่งข้อมูลถ้าเป็นข้อมูล อ่อนไหวจำนวนเงินห้าล้านบาทแล้วคุณต่อจำนวนเคสไปเพราะทั้ง Facebook และ Instagram เริ่มกลัว เนื่องจากการจ่ายเงินไม่ไหว ขอเรียนท่านประธานว่าสามารถดำเนินการได้

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี เพิ่มเติมให้ขอร้องบริษัทว่าเป็นข้อมูลที่ สำคัญที่ dark web นำไปขายให้กับแก๊งคอลเซ็นเตอร์นำไปหลอกลวงประชาชน และเราได้ออกกฎที่แจ้งไปยัง Operator ในเรื่องของการส่ง SMS ถ้า SMS ได้แนบลิงค์ที่เกี่ยวข้องกับการโอนเงินดูดเงินต่าง ๆ เราจะขึ้น ทะเบียนทั้งหมด ใครเป็นผู้ส่งต้องขึ้นทะเบียนทั้งหมดไม่ใช่แค่จ่ายเงินเราจะรู้เซ็ทใหม่จะดำเนินการให้ก่อนปีใหม่ ส่วนนี้จะมีในลักษณะคล้าย ๆ กันทั้ง Facebook Twitter Instagram TikTok คนที่พูดยากที่สุดในประสบการณ์ ของกระทรวงที่เรียกมาคุยคือ Twitter พูดยาก แต่ของบริษัทอื่นยังขอร้องได้แต่ยังไม่อยู่ในเกณฑ์ที่ดี แต่ถ้าเรามี มาตรการในการดำเนินคดีแต่ต้องบอกเขาก่อนว่าถ้าปรากฏแบบนี้ คุณต้องมีส่วนในการรับผิดชอบการออกเงิน ทำเป็นกฎหมายต่าง ๆ เพราะถ้าให้ประชาชนฟ้องก็ไม่ทำเพราะบางทีก็เป็นเรื่องที่ยากลำบาก อาจจะต้องใช้ กฎหมายอื่นเล่นงาน โดยภาครัฐอาจเป็นผู้ฟ้องร้องเพื่อเรียกเงินเรียกค่าเสียหายมาชดเชยเวลา ของผู้เสียหาย เพราะฉะนั้นในเรื่องนี้เป็นประเด็นเรื่องหนึ่งที่หลายท่านได้ให้ข้อสังเกต ๒ เรื่องด้วยกัน เรื่องแรกก็คือขอให้ สืบรวจข้อมูลด้วยเหตุการณ์ที่เกิดความเสียหายให้กับพี่น้องประชาชนในวงกว้าง อาทิเช่น เรื่องของบำเหน็จ บำนาญข้าราชการเรื่องของ เงินค่าประกันมิเตอร์หรือเรื่องอื่น ๆ สืบรวจเรื่องนี้ แล้วก็ประสานงานดำเนินการ แก้ไขปัญหาป้องกันกับหน่วยงานที่เกี่ยวข้อง ให้การป้องกันอัตราความปลอดภัยของข้อมูลมีประสิทธิภาพมาก ยิ่งขึ้น

มติที่ประชุม เห็นชอบรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ประจำปี ๒๕๖๗ (ห้วง ๑ ตุลาคม ๒๕๖๖ - ๓๐ กันยายน ๒๕๖๗) และมอบหมายให้ฝ่ายเลขานุการ นำเสนอคณะรัฐมนตรีเพื่อโปรดทราบต่อไป

๔.๒ ขออนุมัติหลักการมอบหมายให้คณะกรรมการด้านกฎหมาย (กบส.) กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองที่อยู่ในอำนาจหน้าที่ของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พลอากาศตรี อมร ชมเชย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมนางสาวดรุณี พิฤทททอง ผู้อำนวยการสำนักกฎหมาย เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

ข้อกฎหมาย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙ บัญญัติว่า “คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา ๔๒

(๒) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาพความมั่นคงแห่งชาติ

(๔) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐาน การรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

(๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๗) แต่งตั้งและถอดถอนเลขาธิการ

(๘) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุม หรือกำกับดูแลหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(๑๐) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรีเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๑) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๒) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ

(๑๓) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย”

มาตรา ๑๖ บัญญัติว่า “ให้ กกม. มีอำนาจแต่งตั้งคณะอนุกรรมการเพื่อปฏิบัติการ อย่างใดอย่างหนึ่งตามที่ กกม. มอบหมาย”

มาตรา ๒๗ วรรคสอง บัญญัติว่า “ในการปฏิบัติงานตามวรรคหนึ่ง กบส. อาจแต่งตั้ง คณะอนุกรรมการเพื่อพิจารณา เสนอแนะหรือกระทำการอย่างหนึ่งอย่างใดตามที่ กบส. มอบหมายได้ ทั้งนี้ การปฏิบัติงานและการประชุมให้เป็นไปตามหลักเกณฑ์และวิธีการที่ กบส. กำหนด”

ข้อรายงาน/ข้อเท็จจริง

๑. ตามความในมาตรา ๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กมช. มีหน้าที่และอำนาจในการจัดทำนโยบายและแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดมาตรฐานและแนวทางส่งเสริมเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดกรอบการประสานความร่วมมือกับหน่วยงาน รวมทั้งกำหนดกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้อง เป็นสำคัญ แต่อย่างไรก็ตาม กมช. ยังมีหน้าที่และอำนาจที่สำคัญ อีกประการหนึ่งก็คือ การจัดทำกฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่อยู่ในอำนาจหน้าที่ของ กมช. จำนวนทั้งสิ้น ๑๗ ฉบับ ซึ่งปัจจุบันกฎหมายลำดับรอง ทั้ง ๑๗ ฉบับดังกล่าวได้ดำเนินการเรียบร้อยแล้ว

ทั้งนี้ ในการจัดทำกฎหมายลำดับรองดังกล่าวข้างต้น แม้ว่า กมช. จะได้ดำเนินการเรียบร้อยแล้ว แต่ กมช. ยังคงต้องมีการพัฒนา ทบทวน และปรับปรุงกฎหมายลำดับรองแต่ละฉบับ ให้มีความทันสมัยและสอดคล้องกับสภาวะการณ์ที่เปลี่ยนแปลงไปในปัจจุบันอยู่ตลอดเวลา

๒. แม้ว่า กมช. จะมีหน้าที่และอำนาจในการจัดทำกฎหมายลำดับรอง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ แต่ก็สามารถแต่งตั้ง

คณะกรรมการด้านกฎหมายเพื่อทำหน้าที่กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองได้ เนื่องจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มิได้กำหนดเรื่องดังกล่าวไว้ ซึ่งต่างจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ที่มีหน้าที่และอำนาจในการออกกฎหมายลำดับรองเช่นเดียวกับ กมช. แต่สามารถแต่งตั้งคณะกรรมการด้านกฎหมายเพื่อทำหน้าที่กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองได้ โดยอาศัยอำนาจตามมาตรา ๑๖ และมาตรา ๒๗ วรรคสอง แห่งพระราชบัญญัติดังกล่าว

๓. ที่ผ่านมาการเสนอ (ร่าง) กฎหมายลำดับรองที่อยู่ภายใต้ขอบเขตอำนาจของ กมช. นั้น สกมช. จักนำ (ร่าง) กฎหมายลำดับรองแต่ละฉบับเสนอต่อคณะกรรมการด้านกฎหมาย (กบส.) พิจารณาให้ความเห็นชอบขั้นหนึ่งก่อน แล้วจึงเสนอไปยัง กมช. เพื่อพิจารณาให้ความเห็นชอบ ต่อไป ทั้งนี้ การดำเนินการดังกล่าวเป็นไปเพื่อให้คณะกรรมการด้านกฎหมาย (กบส.) ทำหน้าที่กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองแต่ละฉบับให้แก่ กมช. เพื่อให้ (ร่าง) กฎหมายลำดับรองแต่ละฉบับมีความถูกต้องครบถ้วน เหมาะสม และมีประสิทธิภาพ เป็นไปตามเจตนารมณ์ที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๔. สกมช. ขอเรียนว่า เพื่อให้การจัดทำกฎหมายลำดับรองที่อยู่ในอำนาจหน้าที่ของ กมช. เป็นไปด้วยความเรียบร้อย และเพื่อเป็นการมอบหมายให้คณะกรรมการด้านกฎหมาย (กบส.) ทั้งชุดปัจจุบัน และชุดที่จะมีการแต่งตั้งในอนาคต ทำหน้าที่กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองแต่ละฉบับให้แก่ กมช. เพื่อให้ (ร่าง) กฎหมายลำดับรองแต่ละฉบับมีความถูกต้องครบถ้วน เหมาะสม และมีประสิทธิภาพ เป็นไปตามเจตนารมณ์ที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จึงเห็นควรเสนอต่อที่ประชุม กมช. พิจารณามีมติอนุมัติหลักการมอบหมายให้คณะกรรมการด้านกฎหมาย (กบส.) กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองที่อยู่ในอำนาจหน้าที่ของ กมช.

มติที่ประชุม เห็นชอบอนุมัติหลักการมอบหมายให้คณะกรรมการด้านกฎหมาย (กบส.) กลั่นกรองและเสนอความเห็นเกี่ยวกับการจัดทำกฎหมายลำดับรองที่อยู่ในอำนาจหน้าที่ของ กมช.

๔.๓ แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ได้รายงานต่อที่ประชุม โดยมีรายละเอียด ดังนี้

ความเป็นมา

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

เพื่อให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

สาระสำคัญ

ตามอ้างถึง มาตรา ๒๒ (๖) ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจ “เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์” เมื่อวันที่ ๑๖ สิงหาคม ๒๕๖๗ ได้ตรวจพบชื่อผู้ใช้งานและรหัสผ่านหน่วยงานราชการ และมีข้อมูลส่วนบุคคลเป็นจำนวนมาก จากเว็บไซต์ GitLab ที่ URL: <https://gitlab.aitproject.com/anisa/dopa-api/-/blob/master/index.js> จากการตรวจสอบพบว่าเป็นเว็บไซต์ของบริษัทเอกชนรายหนึ่ง ที่รับพัฒนาระบบให้กับหน่วยงานภาครัฐ นั้น

สกมช. ดำเนินการตรวจสอบเหตุการณ์ข้างต้น สรุปเหตุการณ์ได้ดังนี้

๑. จากการตรวจสอบพบว่าสามารถใช้ Credential ดังกล่าวในการเข้าถึงฐานข้อมูล ที่ Host ๒๐๒.๑๗๐.๑๒๐.๑๖๔ ด้วย username: dbo๑_user password: axxx๑๖๔ โดยพบฐานข้อมูลของหน่วยงานราชการและมีข้อมูลส่วนบุคคล ซึ่งมีการจัดเก็บฐานข้อมูลของหน่วยงานราชการและเอกชนพบฐานข้อมูลจำนวน ๑๖๖ ฐานข้อมูล ฐานข้อมูลที่สามารถระบุหน่วยงานได้ จำนวน ๘๑ ฐานข้อมูล เป็นข้อมูลของหน่วยงานราชการ จำนวน ๒๕ หน่วยงาน หน่วยงานเอกชน จำนวน ๘ หน่วยงาน รวมทั้งสิ้น ๓๓ หน่วยงาน และฐานข้อมูลที่ไม่สามารถระบุหน่วยงานได้ จำนวน ๘๕ ฐานข้อมูล

๒. จากการนำ Credential ดังกล่าวในการเข้าถึงระบบของหน่วยงานราชการ โดยพบชื่อผู้ใช้งานและรหัสผ่าน พบว่าสามารถเข้าถึงข้อมูลของหน่วยงานราชการ ดังนี้

๒.๑ พบชื่อผู้ใช้งานและรหัสผ่านระบบของสำนักเลขาธิการนายกรัฐมนตรี จากการตรวจสอบพบว่าสามารถเข้าสู่ระบบของสำนักเลขาธิการนายกรัฐมนตรีได้ แต่ไม่สามารถเข้าถึงฐานข้อมูลได้ เนื่องจากต้องมีการเข้ารหัสระบบผ่านระบบเครือข่ายภายในของสำนักงาน ในเบื้องต้นได้ประสานแจ้งไปยังสำนักเลขาธิการนายกรัฐมนตรี เพื่อลบชื่อผู้ใช้และรหัสผ่าน รวมถึงแก้ไข Username และ Password ในการเข้าถึงฐานข้อมูล

๒.๒ พบชื่อผู้ใช้งานและรหัสผ่านระบบส่งเสริมการมีงานทำของกรมการจัดหางาน สังกัดกระทรวงแรงงาน มีข้อมูล เช่น หมายเลขบัตรประจำตัวประชาชน ชื่อ นามสกุล เบอร์โทร อีเมล เป็นต้น ฐานข้อมูล ๓๓๕.๗ MB ข้อมูลที่จัดเก็บมีมากกว่า ๖๖๐,๐๐๐ คน ในเบื้องต้นได้ประสานแจ้งไปยังกรมการจัดหางาน เพื่อลบชื่อผู้ใช้และรหัสผ่าน รวมถึงแก้ไข Username และ Password ในการเข้าถึงฐานข้อมูล

๒.๓ พบชื่อผู้ใช้งานและรหัสผ่านของกรมการปกครอง สังกัดกระทรวงมหาดไทย มีข้อมูล เช่น หมายเลขบัตรประจำตัวประชาชน ชื่อ นามสกุล เบอร์โทร อีเมล เป็นต้น ฐานข้อมูล ๒๒๑ MB ข้อมูลที่จัดเก็บมีมากกว่า ๔๖๐,๐๐๐ คน ในเบื้องต้นได้ประสานแจ้งไปยังกรมการปกครอง เพื่อลบชื่อผู้ใช้และรหัสผ่าน รวมถึงแก้ไข Username และ Password ในการเข้าถึงฐานข้อมูล

๒.๔ พบชื่อผู้ใช้งานและรหัสผ่าน Data Center ระบบศูนย์ข้อมูลกลางผู้สูงอายุ ของกรมกิจการผู้สูงอายุ สังกัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ โดยมีข้อมูล เช่น หมายเลข บัตรประจำตัวประชาชน ชื่อ นามสกุล เบอร์โทร อีเมล เป็นต้น ขนาดฐานข้อมูล ๒๒๑ MB ข้อมูลที่จัดเก็บ มีมากกว่า ๔๖๐,๐๐๐ คน ในเบื้องต้นประสานหน่วยงานให้ลบชื่อผู้ใช้และรหัสผ่าน รวมถึงแก้ไข Username และ Password ในการเข้าถึงฐานข้อมูล

๓. สภาพปัญหา และสาเหตุการเกิดข้อมูลส่วนบุคคลรั่วไหลจากของหน่วยงานภายใต้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์จากการตรวจพบเข้าถึงฐานข้อมูลที่ Host ๒๐๒.๑๗๐.๑๒๐.๑๖๔ ด้วย username: dbo๐๑_user password: axxx๑๖๔ โดยพบฐานข้อมูลของหน่วยงาน ราชการและมีข้อมูลส่วนบุคคล ซึ่งมีการจัดเก็บฐานข้อมูลของหน่วยงานราชการและเอกชน ได้วิเคราะห์ถึง สาเหตุ สภาพปัญหา และช่องทางการเกิดข้อมูลรั่วไหลจากการที่หน่วยงานของรัฐในประเทศไทยที่ถูกโจมตี เพื่อขโมยข้อมูลส่วนบุคคลไปประกาศขายใน Dark Web หรือเครือข่ายเว็บมืดที่มักถูกใช้เพื่อเข้าถึงข้อมูลผิด กฎหมายโดยอาศัยจุดอ่อนช่องโหว่จากการพัฒนาเว็บไซต์ จุดอ่อนของระบบปฏิบัติการ ก่อให้เกิดความเสียหาย ต่อความน่าเชื่อถือของหน่วยงานของรัฐ โดยสรุปสาระสำคัญได้ ดังนี้

๓.๑ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ ส่วนใหญ่มีการจ้างเอกชนดำเนินการพัฒนาระบบสารสนเทศของหน่วยงานซึ่งไม่มี การกำหนดขอบเขตของงาน (TOR) ให้ครอบคลุมในประเด็นการรักษาความปลอดภัยของข้อมูล รวมทั้งผู้รับจ้าง มักใช้ฐานข้อมูลจริงไปใช้ในขั้นตอนการพัฒนาระบบหลังจากพัฒนาและทดสอบแล้วเสร็จไม่ได้ดำเนินการลบ ข้อมูลดังกล่าว

๓.๒ บริษัทเอกชนที่ไม่ได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ได้มีการปฏิบัติให้เป็นมาตรฐานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และ ไม่ได้ให้ความสำคัญในเรื่องดังกล่าว

๔. สกมช. จึงขอเสนอแนวทางขับเคลื่อนการแก้ไขปัญหาเชิงระบบสำหรับหน่วยงาน ของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อเป็น แนวทาง ในการป้องกันไม่ให้เกิดปัญหาภัยคุกคามทางไซเบอร์ในภาพรวมและการรั่วไหลข้อมูลของหน่วยงาน ดังนี้

๔.๑ การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน ISO/IEC ๒๗๐๐๑ หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ งดใช้ข้อมูลจริงในขั้นตอน การพัฒนาระบบ หรือกำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน รวมทั้ง กำหนดเกณฑ์สำหรับการเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการรับรองทางความ ปลอดภัย ตลอดจนกำหนดให้มีการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใ้ งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๔.๒ หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่อง การออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๔.๓ จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔.๔ กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๔.๕ สร้างระบบเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๔.๖ สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๔.๗ หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าข้อมูลได้

๔.๘ ให้องค์กรยึดหลักตาม Cloud Security Standards และสอดคล้องกับนโยบาย Cloud First Policy เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัล

นายรัชกร ณ ภาพรพิพัฒน์ ผู้แทนเลขาธิการสภาความมั่นคงแห่งชาติ ในเอกสารตามข้อ ๔.๑ ให้องค์กร ควร คำว่า ควร ไม่ใช่ บังคับ

อันที่สองหน่วยงานต่าง ๆ ต้อง ดำเนินการตาม ตาราง ประมวลต่าง ๆ ที่ สกมช ทำอยู่แล้ว ให้สอดคล้อง กับ ISO72001 แต่ IEC72001 แต่ ISO72002 มีกติมากกว่าออกแบบและพัฒนาระบบ

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ชี้แจงเพิ่มเติมว่า ในส่วนนี้ต้องให้มีการนำไปใช้โดยเร่งด่วนเพราะถ้าหากนำเอาข้อความดังกล่าวไปใส่ในระเบียบจัดซื้อจัดจ้าง ก็อาจจะต้องใช้เวลานาน ในตรงนี้อาจใช้เป็นแนวทางเพื่อให้ดำเนินการได้อย่างเร่งด่วน ทั้งนี้ ต้องการให้องค์กรเอาไปใส่ไว้ใน การกำหนด TOR จะมีผลบังคับทางกฎหมาย เพื่อให้เกิดความชัดเจนมากยิ่งขึ้น

นายรัชกร ณ ภาพรพิพัฒน์ ผู้แทนเลขาธิการสภาความมั่นคงแห่งชาติ แสดงความคิดเห็นเพิ่มเติม ถ้าท่านเสนอ ครม. จะมีผลสภาพบังคับใช้ ทุกหน่วยงานจะต้องกำหนดไว้ในขอบเขตของ TOR ในการจัดซื้อจัดจ้าง

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ชี้แจงเพิ่มเติมว่า แต่ในส่วนนี้ถ้าไม่ใช่ คำว่าแนวทางเร่งด่วนจะต้องไปแก้ไขระเบียบจัดซื้อจัดจ้างจะต้องไปผ่านกระบวนการจัดซื้อภาครัฐซึ่งอาจจะต้อง ใช้เวลานาน ไม่ตอบโจทย์กับหน่วยงานรัฐ ในตอนนี้มีภาคเอกชนดำเนินการอยู่แล้วเสนอเป็นการใช้คำว่า แนวทางแต่จะพยายามส่งเสริมให้ทุกหน่วยงานดำเนินการใส่ไว้ใน TOR เพื่อมีไว้บังคับใช้ในสัญญา

พลเรือเอก สุพัต ยูทวงศ์ ผู้แทนรัฐมนตรีว่าการกระทรวงกลาโหม ขอรื้อเรื่องดังนี้ ผมค่อนข้างห่วงใยเช่นเดียวกับท่านรัชกร ณ ภาพรพิพัฒน์ คำว่าแนวทางหรือ Guideline Tool มันอ่อนมาก สภาพบังคับแทบไม่มีอาจจะใช้เป็นหนังสือสั่งการจากรัฐบาลจากคณะรัฐมนตรีหรือเป็นมติ ทุกหน่วยงานดำเนินการ โดยที่ไม่ต้องแก้กฎหมายว่าสามารถดำเนินการได้หรือไม่ เพราะว่าจะมีหลายหน่วยงานทำได้โดยตั้งใจหรือตั้งใจ ก็ตามแต่สุดท้ายแล้วผลเสียก็จะเกิดขึ้นเพราะเราไม่ได้ตรวจ TOR ครบทุกหน่วย

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ลงหารือกับกฤษฎีกา

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ในส่วนนี้ขออนุญาตดำเนินการ พิจารณาเพิ่มเติมกับหน่วยงานที่เกี่ยวข้องให้เป็นมติ ครม. เพื่อให้หน่วยงานของรัฐนำไปใช้ในสัญญากับคำว่า นำไปใช้ซึ่งในส่วนของการดำเนินการนี้จะต้องปรึกษารื้อกับหน่วยงานที่เกี่ยวข้องถึงความเหมาะสม อีกครั้ง สุดท้ายเรายินดีเพราะเป็นเป้าหมายหลักได้เกิดผลบังคับใช้

นายปริญญา หอมอนเก กรรมการผู้ทรงคุณวุฒิฯ แสดงความคิดเห็น ดังนี้ ISO27001 พิมพ์ผิดเป็น ISO/IEC เวอร์ชัน 2022 อาจจะต้องกำหนด และยังมีคำว่าชุดกับแชล ถ้าเป็น ISO27001

จำเป็นจะต้องคือจะต้องทำแต่ถ้าเป็นควรจะเป็น 27002 จะเป็นทำก็ได้ไม่ทำก็ได้อะไรที่ทำใน 2002 ภาพของ ISO บังคับอยู่แล้วเพราะมาตรฐานถ้าเกิดไม่ทำก็ไม่ผ่าน เลยต้องใส่ให้ครบเวอร์ชัน 2022 เพราะว่าเวอร์ชัน 2001 เป็นเวอร์ชันเก่ายังไม่มี PDPA แต่ถ้าเวอร์ชัน 2022 จะมีครบทั้ง cyber ทั้ง privacy

นายรัชกรณ์ นภาพรพิพัฒน์ ผู้แทนเลขาธิการสภาความมั่นคงแห่งชาติ ตั้งข้อสังเกตเวอร์ชัน มั่นมีการปรับเปลี่ยนตามปีเกรงว่าถ้ามีเวอร์ชันใหม่ขอเสนอให้ใช้คำว่าล่าสุดหรือต่ำกว่า

พลอากาศตรี อมร ชมเชย กรรมการและเลขานุการ ขออนุญาตนำเรียนดังนี้ในส่วน of หน่วยงานที่ผ่านจะเป็นสถานภาพของอดีตคือหน่วยงานที่ทำมาแล้วแล้วมีคนมา certify แต่ในประเด็นนี้คือ เป็นระบบงานใหม่ที่เข้ามาเพื่อให้ได้มาตรฐานเดียวกันเพราะฉะนั้นในส่วน of หน่วยงานเดิมทำได้อยู่แล้วเอา ของปีที่แล้วคนมา Audit ในส่วนนี้ จะพูดถึงเรื่องการพัฒนาใหม่เพิ่มเติมทำให้ต้องทำระบบใหม่ให้ได้ตาม มาตรฐานตัวนี้ด้วย

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ผมมีประเด็นหนึ่งในเคสที่เกิดขึ้นเป็นการ เอาข้อมูลเก่าไปรันในระบบ ซึ่งโดยสามัญสำนึกไม่สามารถทำได้อยู่แล้วแต่บริษัทที่รับพัฒนาระบบก็ยัง ดำเนินการทำให้เกิดความเสียหาย เพราะฉะนั้นถ้าจะเพิ่มข้อ ๙ ซึ่งท่านเขียนมาแค่ ๘ ข้อว่าจะเขียนใส่ดีไหม เพิ่มหน้าที่ของการรับผิดชอบในความเสียหายที่เกิดขึ้นจากผู้รับพัฒนาระบบแต่ถ้าใส่ไปคงไม่เป็นอะไร เพราะ ความรับผิดชอบให้เขียนไปเลย เพราะไม่งั้นก็จะเกิดประมาทเลินเล่อฉะนั้นขอให้เพิ่มอีกหนึ่งข้อ เพื่อไม่ให้ บริษัทพัฒนาระบบเกิดความประมาท บังคับให้รู้ว่าจะเอาข้อมูลจริงมารันในระบบเป็นใครแต่ก็ยังผินมาทำ

นายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี ที่ประชุมเห็นชอบและให้เลขาธิการนำ ข้อสังเกตเพิ่มเติมของท่านคณะกรรมการตามที่ให้คำแนะนำไว้

มติที่ประชุม เห็นชอบ แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่ สกมช. เสนอ และมอบหมายให้ สกมช. เสนอแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ให้คณะรัฐมนตรีพิจารณาประกาศให้ ทุกหน่วยงานนำไปใช้งานต่อไป

๔.๔ บันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พลอากาศตรี อมร ชมเชย เลขานุการคณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ แจ้งต่อที่ประชุมขอให้พลตรี ธีรวุฒิ วิทยาภรณ์ รองเลขาธิการคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้รายงานต่อในที่ประชุม โดยมีรายละเอียด ดังนี้

๔.๔.๑ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือทางวิชาการระหว่างสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สถาบันบัณฑิตพัฒนบริหารศาสตร์ โดยคณะนิติศาสตร์

ข้อกฎหมาย

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙ (๖) บัญญัติว่า “คณะกรรมการมีหน้าที่และอำนาจ กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์”

มาตรา ๒๐ บัญญัติว่า “ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น”

มาตรา ๒๒ (๑๒) ได้กำหนดให้ สกมช. มีหน้าที่และอำนาจดังนี้ “ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ”

ข้อรายงาน

ด้วย สกมช. ได้มีความประสงค์จะจัดทำ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือทางวิชาการระหว่างสถาบันบัณฑิตพัฒนบริหารศาสตร์ โดยคณะนิติศาสตร์กับสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อส่งเสริมและสนับสนุนการศึกษาวิจัย และพัฒนาองค์ความรู้ เทคโนโลยี นวัตกรรม และอุตสาหกรรม สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง สรุปได้ดังนี้

๑. บันทึกความเข้าใจด้านการวิจัยและพัฒนา

๑.๑ วัตถุประสงค์

๑.๑.๑ เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความรู้ความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกัน เพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบันสู่ศูนย์กลางการศึกษาในระดับภูมิภาค

๑.๑.๒ ประสานงาน สนับสนุน และให้ความช่วยเหลือสถาบันอุดมศึกษาในเครือข่าย ในการผลิตกำลังคนเฉพาะด้านพัฒนาทักษะรวมทั้งการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๑.๑.๓ ส่งเสริม สนับสนุน พัฒนาปรับปรุงหลักสูตรและดำเนินการในการพัฒนาองค์ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับ การรักษาความมั่นคงปลอดภัยไซเบอร์ ในกลุ่มเป้าหมายบุคลากรของรัฐ ผู้ปฏิบัติงานหน่วยงานท้องถิ่น ผู้ปฏิบัติงานด้านสาธารณสุข บุคลากรด้านการศึกษา เป็นต้น

๑.๑.๔ เพื่อพัฒนาบุคลากรด้านการศึกษาให้มีความพร้อมต่อการถ่ายทอดองค์ความรู้พร้อมดำเนินการขยายผลการพัฒนากลุ่มเป้าหมายให้มีสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากลนำทักษะที่ได้เรียนรู้ไปพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานได้

๑.๑.๕ เพื่อยกระดับสถาบันการศึกษาในระดับพื้นที่สู่การเป็นศูนย์กลางการแลกเปลี่ยนเรียนรู้ ติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๑.๑.๖ ส่งเสริมและสนับสนุนการศึกษาวิจัย และพัฒนาองค์ความรู้ เทคโนโลยี นวัตกรรม และอุตสาหกรรม สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีที่เกี่ยวข้อง

๑.๑.๗ ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรม การบรรยาย การเสวนา การอภิปราย กลุ่ม การประกวดแข่งขัน และกิจกรรมอื่น ๆ เพื่อยกระดับความรู้ ความสามารถ และทักษะความเชี่ยวชาญ ในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชนทั่วไป รวมถึงเจ้าหน้าที่ ในองค์กร นักเรียนและนักศึกษา และผู้ที่เกี่ยวข้องต่อองค์ความรู้

๑.๒ ขอบเขตความร่วมมือ

๒.๑.๑ ความรับผิดชอบร่วมกัน

๑) ให้การสนับสนุนบุคลากรผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล ความมั่นคงปลอดภัยไซเบอร์ ร่วมขับเคลื่อนการพัฒนาการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นผู้เชี่ยวชาญในระดับพื้นที่

๒) ให้มีคณะทำงานเพื่อขับเคลื่อนกิจกรรมด้านความมั่นคง ปลอดภัยไซเบอร์ในระดับพื้นที่ โดยมีองค์ประกอบทั้งหน่วยงานด้านการศึกษา หน่วยงานภาครัฐ และ หน่วยงานภาคีด้านเทคโนโลยี

๓) ให้การสนับสนุนการให้คำปรึกษากับหน่วยงานในระดับ พื้นที่ด้านความมั่นคงปลอดภัยไซเบอร์ และสร้างเครือข่ายเพื่อแลกเปลี่ยนสร้างความเข้มแข็งในระดับพื้นที่

๔) ให้ขับเคลื่อนการพัฒนาทักษะ ความรู้ ความสามารถด้าน ความมั่นคงปลอดภัยไซเบอร์ให้กับ บุคลากรของรัฐ ผู้ปฏิบัติงานหน่วยงานท้องถิ่น ผู้ปฏิบัติงานด้านสาธารณสุข บุคลากรด้านการศึกษา เป็นต้น

๕) ให้การสนับสนุนการทดสอบสมรรถนะด้านความมั่นคง ปลอดภัยไซเบอร์ในระดับสากล เพื่อให้กลุ่มเป้าหมายมีสมรรถนะตามมาตรฐานสากล

๖) ร่วมกันดำเนินงานวิจัยและพัฒนาองค์ความรู้ เทคโนโลยี นวัตกรรม และอุตสาหกรรม ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ในรูปแบบต่าง ๆ ร่วมกันอย่างมี ประสิทธิภาพ รวมทั้งก่อให้เกิดประโยชน์แก่ทั้งสองฝ่าย

๗) ร่วมกันจัดหลักสูตรอบรมและกิจกรรมทางวิชาการ เพื่อเผยแพร่องค์ความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ รายละเอียดความร่วมมือตามบันทึกความเข้าใจข้อ ๒.๑ ถึงข้อ ๒.๗ ทั้งสองฝ่ายจะจัดทำเป็นข้อตกลงโครงการย่อย ภายใต้บันทึกความเข้าใจฉบับนี้ โดยรายละเอียดและข้อตกลง ของโครงการย่อยจะจัดทำในรูปแบบความตกลงเป็นหนังสือของแต่ละโครงการย่อยเป็นรายกรณีไป

๒.๑.๒ รายละเอียดความร่วมมือ

ทั้งสองฝ่ายจะดำเนินการใด ๆ ภายใต้บันทึกความเข้าใจฉบับนี้ให้เป็นไปตาม กฎหมาย กฎ และระเบียบที่เกี่ยวข้อง ในกรณีที่ต้องมีการกำหนดรายละเอียดของการดำเนินการภายใต้ ขอบเขตความร่วมมือตามบันทึกความเข้าใจฉบับนี้ ให้ทั้งสองฝ่ายกำหนดให้มีผู้ประสานงานของแต่ละฝ่าย เพื่อประสานงานและร่วมกันกำหนดรายละเอียดของการดำเนินการในแต่ละเรื่องและนำเสนอผู้มีอำนาจอนุมัติ

ของทั้งสองฝ่ายในการพิจารณาอนุมัติให้ดำเนินการตามหลักเกณฑ์ของแต่ละฝ่ายต่อไป และเมื่อรายละเอียดของการดำเนินการดังกล่าวได้รับอนุมัติแล้ว ให้แต่ละฝ่ายมีหนังสือแจ้งให้อีกฝ่ายหนึ่งทราบ

๒. ขั้นตอนการดำเนินงาน

สภมช. ได้ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือทางวิชาการ เพื่อให้ สถาบันบัณฑิตพัฒนบริหารศาสตร์ พิจารณา ทั้งนี้ หากมีการเปลี่ยนแปลงเนื้อหาที่เป็นสาระสำคัญ จะนำเสนอในที่ประชุมต่อไป

มติที่ประชุม เห็นชอบ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือทางวิชาการระหว่างสถาบันบัณฑิตพัฒนบริหารศาสตร์ โดยคณะนิติศาสตร์ กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมอบหมายให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้ลงนามในบันทึกความเข้าใจว่าด้วยความร่วมมือทางวิชาการระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับสถาบันบัณฑิตพัฒนบริหารศาสตร์ โดยคณะนิติศาสตร์

๔.๔.๒ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมทักษะและการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ มหาวิทยาลัยสวนดุสิต

ข้อรายงาน

ด้วย มหาวิทยาลัยสวนดุสิตได้จัดทำร่างบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมทักษะและการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ มหาวิทยาลัยสวนดุสิต ซึ่งต่อมาได้มีการหารือร่วมกันกับ สำนักงานกฎหมาย และได้กำหนดกรอบการดำเนินงานของแต่ละหน่วยงาน รายละเอียดปรากฏตามเอกสารแนบ

๑. รายละเอียดบันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑.๑ วัตถุประสงค์

๑) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์รวมถึงการสร้างตระหนักรู้ด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกัน เพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

๒) ประสานงาน สนับสนุน และให้ความช่วยเหลือในการผลิตกำลังคนเฉพาะด้านทักษะ รวมทั้งการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๓) ส่งเสริม สนับสนุน และดำเนินการในการพัฒนาองค์ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๔) เพื่อร่วมกันพัฒนาบุคลากรด้านการศึกษาให้มีความพร้อมต่อการถ่ายทอดองค์ความรู้พร้อมดำเนินการขยายผลการพัฒนากลุ่มเป้าหมายให้มีสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากล

๕) ร่วมเป็นหน่วยงานขับเคลื่อน ประสานงานในการดูแลความปลอดภัยทางไซเบอร์และให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ และช่วยเหลือแก้ไขปัญหาให้หน่วยงานต่าง ๆ

๑.๒ ขอบเขตความร่วมมือ

๑) สนับสนุนและส่งเสริมการดำเนินโครงการหรือกิจกรรมทางด้านวิชาการ การพัฒนาบุคลากร การศึกษาแลกเปลี่ยนเรียนรู้ รวมทั้งการเตรียมพร้อมรับการเปลี่ยนแปลงทางเศรษฐกิจ สังคม เทคโนโลยีต่าง ๆ และการเป็นที่ปรึกษาในด้านการบริหารจัดการและพัฒนาองค์กรอย่างยั่งยืน และต่อประเทศโดยรวม

๒) ทั้งสองฝ่ายจะจัดทำข้อตกลงรายละเอียดของการดำเนินงานเป็นแต่ละโครงการหรือกิจกรรมเพิ่มเติมอีกครั้งหนึ่ง หากเห็นว่าบันทึกความเข้าใจฉบับนี้ยังมีเนื้อหาไม่ครบถ้วน โดยจะจัดทำเป็นเอกสารแนบท้ายและให้ถือเป็นส่วนหนึ่งของบันทึกความเข้าใจฉบับนี้

๑.๓ ขั้นตอนการดำเนินงาน

มหาวิทยาลัยสวนดุสิต ได้จัดทำและนำเสนอ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมทักษะและการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ มหาวิทยาลัยสวนดุสิต ให้ สกมช. พิจารณาตรวจสอบ (ร่าง) บันทึกความเข้าใจ และได้ประสานงานกับสำนักกฎหมาย เพื่อปรับแก้ข้อความใน (ร่าง) บันทึกความเข้าใจ มาตามลำดับ

มติที่ประชุม เห็นชอบ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมทักษะและการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ มหาวิทยาลัยสวนดุสิต และมอบหมายให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้ลงนามในบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการส่งเสริมทักษะและการพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกับ มหาวิทยาลัยสวนดุสิต

๔.๔.๓ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์กับ กรมส่งเสริมการเรียนรู้

ข้อรายงาน

ด้วย กรมส่งเสริมการเรียนรู้ ได้จัดทำร่างบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษา

ความมั่นคงปลอดภัยไซเบอร์กับกรมส่งเสริมการเรียนรู้ (สกร.) ซึ่งต่อมาได้มีการหารือร่วมกับสำนักงานกฎหมาย และได้กำหนดกรอบการดำเนินงานของแต่ละหน่วยงาน รายละเอียดปรากฏตามเอกสารแนบ

๑. รายละเอียดบันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑.๑ วัตถุประสงค์

๑) เสริมสร้างความรู้ความเข้าใจแก่บุคลากร นักศึกษา ในสังกัด สกร. ให้ตระหนักรู้ถึงสถานการณ์อาชญากรรมทางไซเบอร์ที่มีผลกระทบต่อประชาชน รวมถึงรูปแบบและวิธีการที่เหล่ามิจฉาชีพ ใช้ในการหลอกลวง และเสริมสร้างการรับรู้เกี่ยวกับมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ที่ถูกต้อง

๒) ส่งเสริมและสนับสนุนหน่วยงานและสถานศึกษาในสังกัด สกร. ในการพัฒนาสมรรถนะ กำลังคน โดยมุ่งเน้นการผลิต พัฒนากำลังคนด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ ให้ได้รับการพัฒนาองค์ความรู้ ทักษะที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อยกระดับศักยภาพของหน่วยงานและสถานศึกษาในสังกัด สกร. ให้มีความพร้อมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๓) ประสานงาน และให้ความช่วยเหลือหน่วยงานและสถานศึกษาในสังกัด สกร. ในการวางแผนปฏิบัติงานตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๔) สนับสนุน ข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานและสถานศึกษาในสังกัด สกร. ตามที่เห็นสมควร

๕) สนับสนุนการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่เห็นสมควร

๖) ติดตาม และเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ และแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๑.๒ ขอบเขตความร่วมมือ

๒.๑.๑ กรมส่งเสริมการเรียนรู้ (สกร.)

๑) ส่งเสริม สนับสนุน และดำเนินการจัดโครงการภายใต้บันทึกความเข้าใจนี้ เพื่อขับเคลื่อนการดำเนินงานในการสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๒) กำหนดแนวทาง และวางแผนการดำเนินงาน ร่วมกับ สกมช. ในการดำเนินการจัดโครงการตามบันทึกข้อตกลงความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๓) อำนวยความสะดวก สนับสนุน และประสานงานระหว่างหน่วยงานและสถานศึกษาในสังกัด สกร. เพื่อพัฒนาความร่วมมือในการสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๔) ทั้งสองฝ่ายจะพัฒนาภาคีเครือข่ายภาคเอกชน เพื่อถ่ายทอดความรู้ ความเข้าใจเกี่ยวกับการสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๕) ให้ข้อเสนอ คำแนะนำ และร่วมกันจัดทำข้อเสนอเชิงนโยบายเพื่อสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๖) วิเคราะห์ รวบรวม สรุปผลการดำเนินงาน และส่งมอบข้อมูลเกี่ยวกับจำนวนหลักสูตร จำนวนบุคลากร ที่ต้องการผลิตกำลังคนด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๗) ส่งเสริม และอบรมให้ความรู้แก่บุคลากรในด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนาศักยภาพและยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๘) ทั้งสองฝ่ายจะติดตาม และประเมินผลการดำเนินงานภายใต้บันทึกข้อตกลงความร่วมมือนี้ ให้เกิดผลอย่างเป็นรูปธรรม และมีประสิทธิผล

๙) ทั้งสองฝ่ายจะประชาสัมพันธ์และเผยแพร่การดำเนินงาน

๒.๑.๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๑) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ให้ความช่วยเหลือหน่วยงานและสถานศึกษาในสังกัด สกร. ในการปฏิบัติตามนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๓) ให้การสนับสนุนในการผลิตกำลังคน พัฒนาทักษะงานวิจัย งานบริการวิชาการ หรืออื่น ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ภายใต้บันทึกข้อตกลงความร่วมมือนี้ ทั้งนี้ให้เป็นไปตามงบประมาณที่ สกมช. ได้รับการจัดสรร

๔) ร่วมมือกับ สกร. ประชาสัมพันธ์และเผยแพร่การดำเนินงาน

๑.๓ ขั้นตอนการดำเนินงาน

กรมส่งเสริมการเรียนรู้ ได้จัดทำและนำเสนอ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ กับ กรมส่งเสริมการเรียนรู้ ให้ สกมช. พิจารณาตรวจสอบ (ร่าง) บันทึกความเข้าใจฯ และได้ประสานงานกับสำนักกฎหมาย เพื่อปรับแก้ข้อความใน (ร่าง) บันทึกความเข้าใจ ฯ มาตามลำดับ

มติที่ประชุม เห็นชอบ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ กับกรมส่งเสริมการเรียนรู้ และมอบหมายให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นผู้ลงนามในบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ กับกรมส่งเสริมการเรียนรู้

๔.๔.๔ (ร่าง) บันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

ข้อรายงาน

ด้วย สกมช. ได้ประสานงานหารือร่วมกับสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) โดยมีความประสงค์ที่จะร่วมกันขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กำหนดนโยบาย มาตรการ รวมทั้งแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการรับมือ ลดความเสี่ยง และสามารถป้องกันภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีเพื่อมิให้เกิดผลกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ จึงได้จัดทำ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ซึ่งมีข้อหารือและได้กำหนดกรอบการดำเนินงานของแต่ละหน่วยงาน สรุปได้ดังนี้

๑. บันทึกความเข้าใจเพื่อสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๑.๑ วัตถุประสงค์

(๑) เพื่อสนับสนุนและส่งเสริมการพัฒนาทักษะความรู้และความตระหนักทราบต่อภัยคุกคามทางไซเบอร์จากการใช้เทคโนโลยีดิจิทัลร่วมกัน เพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน รวมถึงการส่งเสริมความร่วมมือทางวิชาการ งานวิจัย ตลอดจนโครงการพัฒนานวัตกรรมและเทคโนโลยีต่าง ๆ

(๒) เพื่อประสานงาน สนับสนุน ให้คำปรึกษา และให้ความช่วยเหลือในการพัฒนากำลังคนด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ แผนปฏิบัติการ เพื่อสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๓) เพื่อทำงานร่วมกันในการประสานการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ เพื่อติดตาม วิเคราะห์ แก้ไขปัญหา และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๑.๒ หน้าที่ความรับผิดชอบของ สกมช.

(ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กำหนดให้ สกมช. เป็นหน่วยงานผู้รับผิดชอบหลักในการประสานความ

ร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

๒. ขั้นตอนการดำเนินงาน

สภ. ได้จัดทำและนำเสนอ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้ สดช. พิจารณา โดยมีหลักการพิจารณาวัตถุประสงค์ที่เน้นย้ำในเรื่องของความร่วมมือกันส่งเสริมและเพิ่มศักยภาพด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นหลัก ทั้งนี้ ทั้ง ๒ หน่วยงานได้ร่วมกันแก้ไขเนื้อหาสาระสำคัญของ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือฯ จน ทั้ง ๒ หน่วยงานมีความเห็นชอบต่อ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือฯ เป็นที่เรียบร้อยแล้ว

มติที่ประชุม เห็นชอบ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ และมอบหมายให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้ลงนามในบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

๔.๔.๕ (ร่าง) บันทึกความเข้าใจด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ กระทรวงยุติธรรม

ข้อรายงาน

ด้วย สภ. ได้ประสานงานหารือร่วมกับกระทรวงยุติธรรม (ยธ.) โดยมีความประสงค์ที่จะร่วมกันขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีการศึกษาแลกเปลี่ยนองค์ความรู้ พัฒนากำลังคนเฉพาะด้าน เพื่อเตรียมพร้อมรับมือกับการเปลี่ยนแปลงทางเศรษฐกิจ สังคม เทคโนโลยีต่าง ๆ รวมถึงการเป็นที่ปรึกษาในการบริหารจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จึงได้จัดทำ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ กระทรวงยุติธรรม ซึ่งมีข้อหารือและได้กำหนดกรอบการดำเนินงานของแต่ละหน่วยงาน สรุปได้ดังนี้

๑. บันทึกความเข้าใจเพื่อสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๑.๑ วัตถุประสงค์

(๑) เพื่อสนับสนุนและส่งเสริมการพัฒนาทักษะความรู้และความตระหนักรับต่อภัยคุกคามทางไซเบอร์จากการใช้เทคโนโลยีดิจิทัลร่วมกัน เพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะ บูรณาการและเป็นปัจจุบัน รวมถึงการส่งเสริมความร่วมมือทางวิชาการ งานวิจัย ตลอดจนโครงการพัฒนา นวัตกรรมและเทคโนโลยีต่าง ๆ

(๒) เพื่อประสานงาน สนับสนุน ให้คำปรึกษา และให้ความช่วยเหลือในการพัฒนา กำลังคนด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษา ความมั่นคงปลอดภัยทางไซเบอร์ แผนปฏิบัติการ เพื่อสร้างความปลอดภัย การป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์

(๓) เพื่อทำงานร่วมกันในการประสานการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ เพื่อติดตาม วิเคราะห์ แก้ไขปัญหา และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

๒. ขั้นตอนการดำเนินงาน

กระทรวงยุติธรรมได้จัดทำและนำเสนอ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้ สกมช. พิจารณา โดย สกมช. พิจารณาแล้วไม่มีข้อขัดข้องในเนื้อหาสาระสำคัญ โดยพิจารณาวัตถุประสงค์ที่เน้นย้ำในเรื่องของความร่วมมือกันส่งเสริมและเพิ่มศักยภาพด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นหลัก

มติที่ประชุม เห็นชอบ (ร่าง) บันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กับ กระทรวงยุติธรรม และมอบหมายให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นผู้ลงนามในบันทึกความเข้าใจว่าด้วยความร่วมมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กับ กระทรวงยุติธรรม

ระเบียบวาระที่ ๕ เรื่องอื่น ๆ (ถ้ามี)

เลิกประชุมเวลา ๑๑.๔๐ น.

ผู้จัดรายงานการประชุม

พลอากาศตรี 
(ธีรวุฒิ วิทยากรณ์)

ผู้ตรวจรายงานการประชุม

พลอากาศตรี 
(อมร ชมเชย)



ด่วนที่สุด
ที่ กท ๐๒๐๗/๗๖ ๙๕



กระทรวงกลาโหม
ถนนสนามไชย เขตพระนคร
กรุงเทพมหานคร ๑๐๒๐๐

๑๙ มิถุนายน ๒๕๖๘

เรื่อง เสนอความเห็นเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่สำนักเลขาธิการคณะกรรมการรัฐมนตรี ขอให้กระทรวงกลาโหม พิจารณาเสนอความเห็น
ในส่วนที่เกี่ยวข้อง เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ เสนอ เพื่อประกอบการพิจารณาของคณะกรรมการรัฐมนตรี ความละเอียดแจ้งแล้วนั้น

กระทรวงกลาโหม พิจารณาแล้วมีความเห็นว่า กรอบแนวทางการดำเนินการสร้างความมั่นคง
ปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล เป็นการดำเนินการตาม
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และนโยบายของรัฐบาลในการปฏิรูป
ระบบราชการให้มีความทันสมัยสู่การเป็นรัฐบาลดิจิทัล (Digital Government) รวมทั้งมุ่งเน้นการรักษาความมั่นคง
ปลอดภัยด้านไซเบอร์ ควบคู่ไปกับการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลอย่างเป็นระบบ เพื่อลดความเสี่ยง
จากภัยคุกคามทางไซเบอร์ในภาครัฐ อันจะส่งผลให้ระบบดิจิทัลของรัฐบาลมีความมั่นคงปลอดภัยได้มาตรฐานสากลมากขึ้น

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายภูมิธรรม เวชยชัย)

รัฐมนตรีว่าการกระทรวงกลาโหม

สำนักงานปลัดกระทรวงกลาโหม

สำนักนโยบายและแผนกลาโหม

โทร. ๐ ๒๒๒๒ ๙๓๖๙

โทรสาร ๐ ๒๒๒๒ ๙๓๖๙

สำเนาถูกต้อง

พันเอกวิชาญ ศีประเสษฐไชย

(นางสาวปัญญารีย์ ศีประเสษฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด

ที่ กค ๐๒๐๒/๑๖๑๒๒



กระทรวงการคลัง
ถนนพระรามที่ ๖
กรุงเทพฯ ๑๐๔๐๐

๒๙ สิงหาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการรัฐมนตรีขอให้กระทรวงการคลังเสนอความเห็นในส่วนที่เกี่ยวข้องต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เพื่อประกอบการพิจารณาของคณะกรรมการรัฐมนตรีโดยด่วน ความละเอียดแจ้งแล้ว นั้น

กระทรวงการคลังพิจารณาแล้ว ขอเรียนว่า กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ได้กำหนดแนวทางการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันจะส่งผลดีและเป็นประโยชน์ต่อหน่วยงานภาครัฐในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งจะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลในภาครัฐอย่างเป็นระบบและมีความมั่นคงปลอดภัยมากยิ่งขึ้น จึงไม่ขัดข้องในหลักการของกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายพิชัย ชุนทวงษ์)

รัฐมนตรีว่าการกระทรวงการคลัง

สำนักงานปลัดกระทรวงการคลัง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐ ๒๑๒๖ ๕๕๐๐ ต่อ ๓๐๓๐๑
โทรสาร ๐ ๒๒๗๓ ๕๗๕๐

สำเนาถูกต้อง

ปัญญทณีย์ ตีประเสริฐไชย

(นางสาวปัญญทณีย์ ตีประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด

ที่ พม ๐๒๐๙

๐๓๐๖๗



กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๑๐๓๔ ถนนกรุงเกษม แขวงคลองมหานาค
เขตป้อมปราบศัตรูพ่าย กทม. ๑๐๑๐๐

๑๖ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

สิ่งที่ส่งมาด้วย ความเห็นประกอบการพิจารณาของคณะกรรมการรัฐมนตรี จำนวน ๑ ชุด

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการรัฐมนตรี แจ้งขอให้กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เสนอความเห็นต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เพื่อประกอบการพิจารณาของคณะกรรมการรัฐมนตรีความละเอียดแจ้งแล้ว นั้น

กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เห็นด้วยในหลักการตามกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ซึ่งเป็นการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลที่เหมาะสมกับบริบทของภาครัฐที่มีการจัดเก็บข้อมูลส่วนบุคคลจำนวนมาก โดยเฉพาะข้อมูลที่มีความอ่อนไหว อาทิ ข้อมูลสุขภาพ ข้อมูลสวัสดิการ ข้อมูลกลุ่มเปราะบาง ฯลฯ อย่างไรก็ตาม การนำกรอบแนวทางดังกล่าวไปปฏิบัติในหน่วยงานของรัฐจำเป็นต้องได้รับการสนับสนุนตั้งแต่ระดับนโยบาย การจัดสรรงบประมาณ และการเสริมสร้างความเข้าใจให้แก่เจ้าหน้าที่ของรัฐ เพื่อให้บุคลากรทุกระดับมีความตระหนักรู้ต่อการป้องกันและลดความเสี่ยงภัยคุกคามทางไซเบอร์เพื่อให้สามารถดำเนินงานตามภารกิจได้อย่างรัดกุม โปร่งใส และเป็นไปตามหลักธรรมาภิบาลทางดิจิทัล (Digital Governance Principles) และส่งผลให้งานบริการของภาครัฐมีความมั่นคงปลอดภัยยิ่งขึ้น ทั้งนี้ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ มีข้อเสนอแนะเพิ่มเติม เพื่อสนับสนุนการดำเนินการตามกรอบแนวทางดังกล่าวในการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลอย่างเป็นระบบและมีประสิทธิภาพ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายวรารุณ ศิลปอาษา)

รัฐมนตรีว่าการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

สำเนาถูกต้อง

สำนักงานปลัดกระทรวงฯ
กองยุทธศาสตร์และแผนงาน
โทร. ๐ ๒๖๕๕ ๖๔๔๔
โทรสาร ๐ ๒๖๕๕ ๖๔๔๘

ชัญญกานต์ ศิปปะเสริญไชย
(นางสาวปัญฑารีย์ ศิปปะเสริญไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

**ความเห็นประกอบการพิจารณาของคณะรัฐมนตรี
ของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์**

ต่อ

**กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล**

กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เห็นด้วยในหลักการตามกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ซึ่งเป็นการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลที่เหมาะสมกับบริบทของภาครัฐที่มีการจัดเก็บข้อมูลส่วนบุคคลจำนวนมาก โดยเฉพาะข้อมูลที่มีความอ่อนไหว อาทิ ข้อมูลสุขภาพ ข้อมูลสวัสดิการ ข้อมูลกลุ่มเปราะบาง ฯลฯ อย่างไรก็ตาม การนำกรอบแนวทางดังกล่าวไปปฏิบัติในหน่วยงานของรัฐ จำเป็นต้องได้รับการสนับสนุนตั้งแต่ระดับนโยบาย การจัดสรรงบประมาณ และการเสริมสร้างความเข้าใจให้แก่เจ้าหน้าที่ของรัฐ เพื่อให้บุคลากรทุกระดับมีความตระหนักต่อการป้องกันและลดความเสี่ยงภัยคุกคามทางไซเบอร์ เพื่อให้สามารถดำเนินงานตามภารกิจได้อย่างรัดกุม โปร่งใส และเป็นไปตามหลักธรรมาภิบาลทางดิจิทัล (Digital Governance Principles) และส่งผลให้งานบริการของภาครัฐมีความมั่นคงปลอดภัยยิ่งขึ้น ทั้งนี้ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ มีข้อเสนอแนะเพิ่มเติม เพื่อสนับสนุนการดำเนินการตามกรอบแนวทางดังกล่าวในการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลอย่างเป็นระบบและมีประสิทธิภาพ ดังนี้

๑. การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงาน ควรกำหนดให้มีการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment : PIA) ก่อนเริ่มพัฒนาระบบที่มีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล เพื่อประเมินประเภทของข้อมูลที่จัดเก็บ สิทธิการเข้าถึง และความเสี่ยงที่อาจเกิดขึ้น พร้อมทั้งควรกำหนดให้ใช้ข้อมูลจำลองแทนข้อมูลจริงในการทดสอบ และลบออกภายใน ๓ วันหลังจบแต่ละรอบการทดสอบ เพื่อป้องกันความเสี่ยงจากการตกค้างของข้อมูล นอกจากนี้ ควรเพิ่มกระบวนการตรวจสอบความปลอดภัยของรหัสต้นทาง (Source code) และการสแกนช่องโหว่ (Static Application Security Testing : SAST) ก่อนนำระบบขึ้นใช้งานจริง โดยต้องไม่มีช่องโหว่ในระดับที่มีความรุนแรงสูงสุดตามมาตรฐาน Common Vulnerability Scoring System หรือ CVSS และกำหนดให้ขอบเขตของงาน (Terms of Reference : TOR) ของผู้พัฒนาต้องผ่านการรับรองมาตรฐานด้านความมั่นคงปลอดภัย อาทิ ISO/IEC 27001 NIST CSF ฯลฯ

๒. การอบรมและสร้างความรู้ความเข้าใจแก่บุคลากร ควรจัดอบรมเฉพาะด้านให้แก่ผู้พัฒนาในเรื่อง แนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) โดยครอบคลุมเนื้อหาหลัก เช่น การตรวจสอบข้อมูลนำเข้า การออกแบบการยืนยันตัวตนที่ปลอดภัย เป็นต้น พร้อมมีแบบทดสอบหลังอบรม และออกใบรับรองที่มีการต่ออายุทุกปี เพื่อรักษามาตรฐานวิชาชีพอย่างต่อเนื่อง สำหรับบุคลากรทั่วไปควรได้รับการอบรมเรื่อง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) เพื่อให้เข้าใจบทบาทหน้าที่ของตนเอง การขอความยินยอม และสิทธิของเจ้าของข้อมูล

๓. การตรวจสอบและประเมินผลระบบ ควรกำหนดให้มีการประเมินความปลอดภัยของระบบอย่างสม่ำเสมอ โดยเฉพาะระบบที่มีความเสี่ยงสูง เช่น ระบบฐานข้อมูลประชาชน เป็นต้น ซึ่งควรให้มีการประเมินอย่างน้อยเป็นรายไตรมาส ส่วนระบบทั่วไปควรประเมินทุก ๖ เดือน และควรกำหนดเกณฑ์การยอมรับความเสี่ยง (Risk Acceptance Criteria) อย่างชัดเจน เช่น ไม่อนุญาตให้นำระบบที่มีช่องโหว่ระดับที่มีความรุนแรงสูงสุด (CVSS $\geq$ 9.0) ไปใช้งานจริงในระบบ Production

๔. การกำหนด...

๔. การกำหนดเงื่อนไขในสัญญาว่าจ้างผู้พัฒนาระบบ ควรกำหนดเงื่อนไขด้านความมั่นคงปลอดภัยในสัญญาว่าจ้างอย่างชัดเจน รวมถึงบทลงโทษในกรณีเกิดการรั่วไหลของข้อมูล เช่น ค่าปรับต่อรายต่อเหตุการณ์ เป็นต้น เพื่อสร้างแรงจูงใจให้เกิดความรับผิดชอบต่อข้อมูลภาครัฐ นอกจากนี้ ผู้รับจ้างควรมีประกันภัยด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Liability Insurance) เพื่อรับมือกับความเสียหายที่อาจเกิดขึ้น และควรระบุสิทธิของหน่วยงานในการตรวจสอบกระบวนการพัฒนา (Right to Audit)

๕. การใช้งานระบบคลาวด์อย่างมั่นคงปลอดภัย ซึ่งนอกจากการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ซึ่งสอดคล้องกับนโยบาย Cloud First Policy แล้ว ก่อนย้ายข้อมูลขึ้นระบบคลาวด์ ควรมีการประเมินความเสี่ยง (Cloud Security Assessment) และจัดให้มีระบบติดตามและตรวจสอบการใช้งานระบบคลาวด์อย่างต่อเนื่อง พร้อมทั้งกำหนดข้อกำหนดที่ตั้งข้อมูล (Data Residency Requirements) สำหรับข้อมูลที่อ่อนไหว อาทิ ข้อมูลสุขภาพ ข้อมูลสวัสดิการ ฯลฯ ให้จัดเก็บภายในประเทศหรือในเขตเศรษฐกิจที่มีข้อตกลงร่วมกับประเทศไทย

๖. การจัดการข้อมูลส่วนบุคคลในเชิงระบบ ควรจัดทำแผนภาพแสดงการไหลของข้อมูล (Data Flow Mapping) เพื่อให้เข้าใจว่าข้อมูลไหลไปถึงผู้ใดบ้าง และบุคคลระดับใดมีสิทธิ์เข้าถึงหรือรับผิดชอบข้อมูลในแต่ละช่วง นอกจากนี้ ควรกำหนดนโยบายการเก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น (Data Minimization) และกำหนดระยะเวลาเก็บข้อมูลที่ชัดเจน (Data Retention) เพื่อลดความเสี่ยงและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) อีกทั้งควรมีกระบวนการที่รองรับการใช้สิทธิ์ของเจ้าของข้อมูล (Data Subject Rights Management) อาทิ การขอแก้ไขข้อมูล ฯลฯ ได้อย่างสะดวกและปลอดภัย

ด่วนที่สุด

ที่ ดศ ๐๑๐๐.๔/๒๔๘



กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา
อาคารซี ซอยแจ้งวัฒนะ ๗ ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๒๕ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการ

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการ ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการขอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอความเห็นในส่วนที่เกี่ยวข้องเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล เพื่อประกอบการพิจารณาของคณะกรรมการ ความละเอียดแจ้งแล้ว นั้น

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาแล้ว ไม่มีข้อขัดข้องในหลักการต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เนื่องจากเป็นการกำหนดแนวปฏิบัติสำคัญเพื่อยกระดับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ในการป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของหน่วยงานของรัฐอย่างเป็นระบบ ซึ่งจะมีส่วนสำคัญในการเสริมสร้างเสถียรภาพของระบบดิจิทัลของหน่วยงานของรัฐและความเชื่อมั่นของประชาชนในภาพรวม ทั้งนี้ กรอบแนวทางดังกล่าวยังมีความสอดคล้องกับมาตรฐานสากลและสนับสนุนการดำเนินงานตามนโยบายการใช้คลาวด์เป็นหลักของรัฐบาล อย่างไรก็ดี เพื่อให้การนำกรอบแนวทางดังกล่าวไปสู่การปฏิบัติอย่างเคร่งครัดและเป็นรูปธรรม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเห็นควรให้มีการกำหนดกลไกในการติดตาม ตรวจสอบ และประเมินผลอย่างต่อเนื่อง เพื่อนำมาปรับปรุงและพัฒนาแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้สามารถรับมือกับสถานการณ์และภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว อันจะนำไปสู่ระบบดิจิทัลของหน่วยงานของรัฐที่มีความมั่นคงปลอดภัย และสร้างความเชื่อมั่นให้กับประชาชนอย่างแท้จริง

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายประเสริฐ จันทรรวงทอง)

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำเนาถูกต้อง

สำนักงานปลัดกระทรวง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

โทรศัพท์ ๐ ๒๑๔๑ ๖๕๐๘

ไปรษณีย์อิเล็กทรอนิกส์ saraban@mdes.go.th

ศษฎาภรณ์ คีประเสริฐไชย

(นางสาวปัญญารีย์ ตีประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด
ที่ รง ๐๒๐๑.๒/๒๓๒๗



กระทรวงแรงงาน
ถนนมิตรไมตรี ดินแดง
กรุงเทพมหานคร ๑๐๔๐๐

๑๗ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการรัฐมนตรีขอให้กระทรวงแรงงานพิจารณาเสนอความเห็น
ในส่วนที่เกี่ยวข้อง เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ของสำนักงานคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ เพื่อประกอบการพิจารณาของคณะกรรมการรัฐมนตรี ความละเอียดแจ้งแล้ว นั้น

กระทรวงแรงงานพิจารณาแล้ว ไม่ขัดข้องต่อกรอบแนวทางการดำเนินการสร้างความมั่นคง
ปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เนื่องจากกรอบแนวทางดังกล่าว
จะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ
ทำให้บริการของภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายพงศ์กวิน จึงรุ่งเรืองกิจ)

รัฐมนตรีว่าการกระทรวงแรงงาน

สำนักงานปลัดกระทรวง

กองกลาง

โทรศัพท์ ๐ ๒๒๓๒ ๑๑๕๗

ไปรษณีย์อิเล็กทรอนิกส์ saraban.mol@mol.mail.go.th

สำเนาถูกต้อง

ปัญญาวิช กัประเสฐจุไชย

(นางสาวปัญฑารีย์ ดิประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด

ที่ ศธ ๐๒๐๒.๒/ ๑๕๕๕



กระทรวงศึกษาธิการ

กทม. ๑๐๓๐๐

๑๗ มิถุนายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการรัฐมนตรีขอให้กระทรวงศึกษาธิการเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ความละเอียดแจ้งแล้ว นั้น

กระทรวงศึกษาธิการ พิจารณาแล้ว เพื่อเป็นการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคล และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของหน่วยงานมีความมั่นคงปลอดภัยมากยิ่งขึ้น จึงเห็นด้วยกับกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล และดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

พลตำรวจเอก

(เพิ่มพูน ชิดชอบ)

รัฐมนตรีว่าการกระทรวงศึกษาธิการ

สำนักงานปลัดกระทรวง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

โทรศัพท์ ๐ ๒๒๘๑ ๒๗๑๒

โทรสาร ๐ ๒๒๘๑ ๘๒๑๘

E-mail: sarabun_bict@moe.go.th

สำเนาถูกต้อง

ณัฐกานต์ กิ่งประเสริฐไชย

(นางสาวปัญฑารีย์ ดีประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

“เรียนดี มีความสุข”

- 2 ก.ย. 2568

ที่ สธ ๐๒๑๒/๒๓๕๐



กระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๓ มิถุนายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ขอให้กระทรวงสาธารณสุขให้ความเห็น
ในส่วนที่เกี่ยวข้อง เพื่อประกอบการพิจารณาของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ประเด็นความเห็น เรื่อง กรอบแนวทาง
การดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคล
ไม่ให้เกิดการรั่วไหล ความละเอียดแจ้งแล้ว นั้น

กระทรวงสาธารณสุข พิจารณาแล้วมีความเห็นว่าเพื่อให้หน่วยงานภายใต้สังกัดกระทรวงสาธารณสุข
ซึ่งมีการเก็บ รวบรวม ใช้ และประมวลผลข้อมูลสุขภาพส่วนบุคคล มีแนวทางปฏิบัติในการสร้างความมั่นคง
ปลอดภัยไซเบอร์สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลอย่างเป็นรูปธรรมและเป็นไป
ตามมาตรฐานสากล อาทิ ISO/IEC 27001 หรือ NIST Cyber Security Framework จึงเห็นชอบในหลักการของ
กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูล
ส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

จึงเรียนมาเพื่อโปรดพิจารณาและดำเนินการต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายสมศักดิ์ เทพสุทิน)

รัฐมนตรีว่าการกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

โทร. ๐ ๒๕๕๐ ๑๒๑๓

ไปรษณีย์อิเล็กทรอนิกส์ saraban0212@moph.go.th

สำเนาถูกต้อง

ปัญญากิจ กัปรัสสิริไชย

(นางสาวปัญญารีย์ ตีประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568



ที่ นร ๐๕๐๘/ ๗๔๕๗

สำนักเลขาธิการนายกรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง ขอให้สำนักเลขาธิการนายกรัฐมนตรีเสนอความเห็นเพื่อประกอบการพิจารณาของคณะกรรมการรัฐมนตรี เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ ความละเอียดแจ้งแล้ว นั้น

สำนักเลขาธิการนายกรัฐมนตรีพิจารณาแล้ว เห็นด้วยในหลักการข้อเสนอของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เนื่องจากการยกระดับมาตรการป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของหน่วยงานภาครัฐ ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบต่อความเชื่อมั่นและความมั่นคงของประเทศ เพื่อให้มีมาตรฐานทัดเทียมกับระดับสากล ส่งผลให้บริการภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น โดยมีข้อเสนอสำหรับประกอบการดำเนินการเพิ่มเติม ดังนี้

๑. ควรมีการจัดทำทะเบียนรายชื่อผู้รับจ้างที่มีคุณสมบัติและความเชี่ยวชาญด้านความปลอดภัยไซเบอร์ที่เชื่อถือได้ เพื่อเป็นแหล่งข้อมูลให้หน่วยงานภาครัฐใช้ประกอบการพิจารณาเลือกผู้รับจ้างพัฒนาระบบ ทั้งนี้ เพื่อเป็นการกำกับดูแลและตรวจสอบผู้รับจ้างให้มีการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่กำหนดอย่างเคร่งครัด

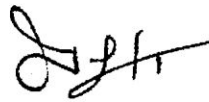
๒. ควรมีกฎและเครื่องมือ (Toolkit) ให้หน่วยงานของรัฐสามารถนำไปใช้ในการตรวจสอบความมั่นคงปลอดภัยของระบบอย่างต่อเนื่อง (Regular Security Audit) เพื่อประเมินจุดอ่อน/จุดเสี่ยงและหาทางปรับปรุงแก้ไขได้ทันที่ รวมทั้งควรมีระบบสำหรับแลกเปลี่ยนข้อมูลและเผยแพร่บทเรียนจากเหตุการณ์ความปลอดภัยไซเบอร์ เพื่อแจ้งเตือนและเตรียมพร้อมสำหรับป้องกันและจัดการกับภัยคุกคามที่คล้ายคลึงกัน

/ศ. ควรส่งเสริม...

๓. ควรส่งเสริมให้หน่วยงานของรัฐสร้างวัฒนธรรมความปลอดภัยไซเบอร์ โดยในระดับองค์กร ควรมีการกำหนดเป็นตัวชี้วัด (KPI) ให้ทุกหน่วยงาน โดยเฉพาะหน่วยงานที่ได้รับการประเมินตรวจสอบว่ามีความเสี่ยงต่อภัยคุกคามด้านไซเบอร์และการรั่วไหลของข้อมูลส่วนบุคคลต้องมีการจัดทำแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์ (Incident Response Plan) ส่วนในระดับบุคคล สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานพัฒนารัฐบาลดิจิทัล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ควรมีการพัฒนาบุคลากรเพื่อสร้างความตระหนักรู้และจิตสำนึกเกี่ยวกับภัยคุกคามทางไซเบอร์ และการปกป้องคุ้มครองข้อมูลส่วนบุคคลให้กับบุคลากรทุกระดับของหน่วยงานภาครัฐอย่างต่อเนื่อง

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ



(นายพรหมินทร์ เลิศสุริย์เดช)

เลขาธิการนายกรัฐมนตรี

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

โทร. ๐ ๒๒๘๘ ๔๐๐๐ ต่อ ๔๔๐๖

ไปรษณีย์อิเล็กทรอนิกส์ : saraban@thaigov.go.th

สำเนาถูกต้อง

ปัญญาภรณ์ ศีประเสริญไชย

(นางสาวปัญญาภรณ์ ศีประเสริญไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด

ที่ นร ๐๗๐๘/วส๕

สำนักงบประมาณ

๑๐๖๓ ถนนพหลโยธิน

แขวงพญาไท กรุงเทพฯ ๑๐๕๐๐

๒๙ สิงหาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔

ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะกรรมการรัฐมนตรีขอให้สำนักงบประมาณเสนอความเห็น
ในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะกรรมการรัฐมนตรี กรณีคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติเสนอเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์
ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล เพื่อให้คณะกรรมการพิจารณา ดังนี้

๑. เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงาน
ของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

๒. อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์
ให้กับระบบงานของหน่วยงานต่อไป

ความละเอียดแจ้งแล้ว นั้น

สำนักงบประมาณพิจารณาแล้วขอเรียนว่า กรอบแนวทางการดำเนินการสร้างความมั่นคง
ปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล
มีวัตถุประสงค์เพื่อขับเคลื่อนการแก้ไขปัญหาเชิงระบบสำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล
และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อาทิ การกำหนดขอบเขตของงานพัฒนาระบบ
หน่วยงานที่มีมาตรฐาน จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ ตลอดจน
จัดอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย ส่งผลให้
ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัย เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน
ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มีมติเห็นชอบแนวทางดังกล่าว ในคราวประชุม
ครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ แล้ว จึงเห็นสมควรที่คณะกรรมการรัฐมนตรีจะพิจารณาให้ความเห็นชอบ

/ในหลักการ...

ในหลักการแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล และอนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ สำหรับค่าใช้จ่ายที่จะเกิดขึ้น เห็นควรให้หน่วยงานที่เกี่ยวข้องใช้จ่ายจากงบประมาณรายจ่ายประจำปีที่ได้รับจัดสรร หรือพิจารณาปรับแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ โดยโอนงบประมาณรายจ่าย โอนเงินจัดสรรหรือเปลี่ยนแปลงเงินจัดสรร ตามระเบียบว่าด้วยการบริหารงบประมาณ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม แล้วแต่กรณี หรือจัดทำแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ เพื่อเสนอขอตั้งงบประมาณรายจ่ายประจำปีตามความจำเป็นและเหมาะสมตามขั้นตอนต่อไป

จึงเรียนมาเพื่อโปรดนำเสนอความเห็นประกอบการพิจารณาของคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ



(นายอนันต์ แก้วกำเนิด)

ผู้อำนวยการสำนักงบประมาณ

กองจัดทำงบประมาณด้านเศรษฐกิจ ๓

โทร. ๐ ๒๒๗๘ ๗๐๐๐ ต่อ ๑๒๗๑

ไปรษณีย์อิเล็กทรอนิกส์ saraban@bb.go.th

สำเนาถูกต้อง

ปัญญาภรณ์ คีประเสริฐไชย

(นางสาวปัญญาภรณ์ คีประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

ด่วนที่สุด

ที่ นร ๐๕๐๙/๘๘



สำนักงานคณะกรรมการกฤษฎีกา
๑ ถนนพระอาทิตย์ เขตพระนคร
กรุงเทพฯ ๑๐๒๐๐

๓๐ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔
ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้สำนักงานคณะกรรมการกฤษฎีกาเสนอความเห็นในส่วนที่เกี่ยวข้องกับเรื่องดังกล่าวตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เสนอ เพื่อประกอบการพิจารณาของคณะรัฐมนตรีโดยด่วนความละเอียดทราบแล้ว นั้น

สำนักงานคณะกรรมการกฤษฎีกาพิจารณาแล้ว เห็นว่า กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอต่อคณะรัฐมนตรี เพื่อพิจารณาให้ความเห็นชอบและขออนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป เป็นการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเสนอแนะและให้ความเห็นต่อคณะรัฐมนตรีเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ (๑๐) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรณีจึงเป็นอำนาจของคณะรัฐมนตรีที่จะพิจารณาให้ความเห็นชอบและอนุมัติตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอได้ตามที่เห็นสมควร

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายปรกรณ์ นิลประพันธ์)

เลขาธิการคณะกรรมการกฤษฎีกา

กองกฎหมายเทคโนโลยีและการคมนาคม
ฝ่ายกฎหมายเทคโนโลยีและการพลังงาน
โทร. ๐ ๒๒๒๒ ๐๒๐๖ - ๙ ต่อ ๑๑๔๓ (นายธิตา)
โทรสาร ๐ ๒๒๒๖ ๖๒๐๑
www.ocs.go.th
www.lawreform.go.th
ไปรษณีย์อิเล็กทรอนิกส์ saraban@ocs.go.th

สำเนาถูกต้อง

ณัฐทาร์ช คีประเสริฐไชย

(นางสาวปัญฑารีย์ คีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568



ที่ นร ๑๑๑๖/๒๕๕๓

สำนักงานสภาพัฒนาการ
เศรษฐกิจและสังคมแห่งชาติ
๙๖๒ ถนนกรุงเกษม กรุงเทพฯ ๑๐๑๐๐

๑๗ มิถุนายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการ
การป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการ

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการ ส่วนที่สี่ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่สำนักเลขาธิการคณะกรรมการขอให้สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
เสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะกรรมการ เรื่อง กรอบแนวทางการ
ดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคล
ไม่ให้เกิดการรั่วไหล ที่เสนอโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงาน
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ความละเอียดแจ้งแล้วนั้น

สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติพิจารณาแล้ว มีความเห็นดังนี้

๑. เห็นควรให้ความเห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์
ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลและอนุมัติให้ทุกหน่วยงานนำไป
ดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป

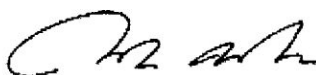
๒. สกมช. ควรสร้างความรู้ความเข้าใจในการพิจารณาประยุกต์ใช้มาตรฐาน ISO/IEC ๒๗๐๐๑
หรือ NIST Cyber Security Framework สำหรับหน่วยงานรัฐในการกำหนดขอบเขตของงานพัฒนาระบบ
โดยเน้นหัวข้อที่มีลำดับความสำคัญก่อนเพื่อให้หน่วยงานรัฐมีระยะเวลาในการเตรียมความพร้อมและจัดหา
งบประมาณ และหารือกับสำนักงบประมาณในการพิจารณาจัดสรรงบประมาณให้หน่วยงานที่เกี่ยวข้องให้
เหมาะสมสำหรับการบริหารจัดการความเสี่ยงในการจัดทำโครงการพัฒนาระบบและการฝึกอบรมพัฒนา
บุคลากรด้านเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐได้อย่างเหมาะสมและเกิดประสิทธิภาพ นอกจากนี้
ควรมีแนวทางที่ยืดหยุ่นและการสนับสนุนที่เหมาะสมในการกำหนดเกณฑ์ให้บริษัทพัฒนาซอฟต์แวร์
มีมาตรฐานที่ผ่านการรับรองทางความปลอดภัย เพื่อให้กลุ่มธุรกิจ Startup และผู้ประกอบการ SMEs
เตรียมความพร้อมก่อนมีการบังคับใช้กรอบแนวทางดังกล่าว ซึ่งจะเป็นการสนับสนุนภาคธุรกิจขนาดกลางและ

/ขนาดย่อม...

ขนาดย่อมให้สามารถดำเนินธุรกิจได้อย่างยั่งยืน อีกทั้งหน่วยงานภาครัฐที่ได้รับจำนวนเงินงบประมาณสนับสนุน
โครงการพัฒนาระบบที่ไม่สูงมากหรือตั้งอยู่ในหน่วยงานส่วนภูมิภาคสามารถสรรหาผู้รับจ้างในกลุ่มผู้ประกอบการ
วิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ได้

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ



(นายดนุชา พิชนันท์)

เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

โทร. ๐ ๒๒๘๐ ๔๐๘๕ ต่อ ๕๔๐๑

E-mail : Archan@nesdc.go.th

สำเนาถูกต้อง

ปัญญาภรณ์ คีปะเสงิจูโซ

(นางสาวปัญฑารีย์ ดีประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

ด่วนที่สุด

ที่ สพร ๒๕๖๘/๑๕๙๐

๒๗ พฤษภาคม ๒๕๖๘

เรื่อง ตอบกลับกรอบแนวทางการดำเนินการความปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะกรรมการรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะกรรมการรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔
ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่อ้างถึง สำนักงานคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง
กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกัน
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล โดยกองวิเคราะห์เรื่องเสนอคณะรัฐมนตรี มีการสอบถามความเห็น
ในส่วนรายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๗
วาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับป้องกันข้อมูลส่วนบุคคลรั่วไหล สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้ข้อมูลรั่วไหล มีรายละเอียด
การป้องกัน ๘ รายการ ดังนี้

๑. การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน
ISO/IEC 27001 หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ งดใช้ข้อมูลจริงในขั้นตอน
การพัฒนาระบบ หรือกำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน
รวมทั้ง กำหนดเกณฑ์สำหรับการเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการ
รับรองทางความปลอดภัยตลอดจนกำหนดให้มีการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วง
การพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒. หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่อง การออกแบบ
และพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓. จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึง
การตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔. กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้น
ความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕. สร้างระบบเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่ เกิดขึ้น
อย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖. สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์ และแพตช์
ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗. หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

๘. ให้หน่วยงานยึดหลักตาม Cloud Security Standards และสอดคล้องกับนโยบาย
Cloud First Policy เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัล

ในการนี้ สำนักงาน...

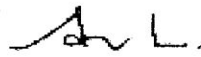
ในการนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มีความเห็นในข้อ ๑ ดังนี้

๑. “การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน ISO/IEC 27001 หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ” สำนักงานเห็นว่าควรให้ความชัดเจนในประเด็นนี้ ในส่วนของงานที่มีการจ้างพัฒนาจากภายนอกหรือหน่วยงานรัฐจำเป็นต้องผ่านการรับรองมาตรฐาน ISO/IEC 27001 ในงานที่เกี่ยวข้องในการพัฒนาออกแบบหรือไม่ เพราะจะมีผลต่อการขอใบรับรอง และเกิดค่าใช้จ่ายของหน่วยงานรัฐ หรือหน่วยงานภายนอกที่ต้องดำเนินการ

๒. “กำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน” สำนักงานเห็นว่า ควรมีการระบุความชัดเจนของข้อความที่ครอบคลุมถึงวิธีการลบ หรือทำลายที่ปลอดภัย พร้อมระบุให้ทวนสอบการลบข้อมูลหรือทำลาย ว่าข้อมูลไม่สามารถนำกลับมาใช้งานได้

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ



(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการ รักษาการแทน

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ฝ่ายความมั่นคงปลอดภัยไซเบอร์

ส่วนแผนงานและที่ปรึกษาความมั่นคงปลอดภัยไซเบอร์

มือถือ ๐๘ ๐๐๔๕ ๓๑๖๓ (ศรีสุตา)

ไปรษณีย์อิเล็กทรอนิกส์ cbp_division@dga.or.th

ไปรษณีย์อิเล็กทรอนิกส์สารบรรณกลาง saraban@dga.or.th

สำเนาถูกต้อง

ปัญญาวิช กัปประเสริฐไชย

(นางสาวปัญญาวิช กัปประเสริฐไชย)

นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568