ที่ นร ๐๕๐๖/๙๕๑๙

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๑๗ มกราคม ๒๕๕๖

เรื่อง ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ เรื่อง การบริหารจัดการระบบการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ

เรียน เลขาธิการสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ที่ สศ ๐๐๐๑/๑๕๘๕ ลงวันที่ ๔ กันยายน ๒๕๕๕

สิ่งที่ส่งมาด้วย สำเนาหนังสือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ด่วนที่สุด ที่ ทก ๐๑๐๐.๔/๑๑๔๙๘ ลงวันที่ ๙ พฤศจิกายน ๒๕๕๕

ตามที่ได้เสนอความเห็นและข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ เรื่อง การบริหารจัดการระบบการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ ไปเพื่อดำเนินการความละเอียดแจ้งแล้ว นั้น

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้เสนอผลการพิจารณาและผลการดำเนินการร่วมกับหน่วยงานที่เกี่ยวข้อง ไปเพื่อประกอบการพิจารณาของคณะรัฐมนตรีด้วย ความละเอียดปรากฏตามสำเนาหนังสือที่ส่งมาด้วยนี้

คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๑๕ มกราคม ๒๕๕๖ ว่า

๑ รับทราบความเห็นและข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ

๒ รับทราบความเห็น ผลการพิจารณา และผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับกระทรวงกลาโหม กระทรวงยุติธรรม กระทรวงวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ สำนักงานปลัดสำนักนายกรัฐมนตรี สำนักข่าวกรองแห่งชาติ สำนักงบประมาณ สำนักงานสภาความมั่นคงแห่งชาติ สำนักงานคณะกรรมการกฤษฎีกา สำนักงาน ก.พ. สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) และสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ

จึงเรียนมาเพื่อโปรดทราบ ทั้งนี้ สำนักเลขาธิการคณะรัฐมนตรีได้แจ้งให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารทราบด้วยแล้ว และได้เผยแพร่ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติพร้อมความเห็นและผลการพิจารณาของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารทางเว็บไซต์ของสำนักเลขาธิการคณะรัฐมนตรีเพื่อให้สาธารณชนได้รับทราบ และขอขอบคุณสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติที่ให้ความเห็นและข้อเสนอแนะในเรื่องดังกล่าวต่อคณะรัฐมนตรี

ขอแสดงความนับถือ

(นายอำพน กิตติอำพน)
เลขาธิการคณะรัฐมนตรี
17 ม.ค. 2556

สำนักวิเคราะห์เรื่องเสนอคณะรัฐมนตรี
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๓๒๓
โทรสาร ๐ ๒๒๘๐ ๙๐๖๔ www.cabinet.thaigov.go.th (R27-01-56 : นิสา)

รอง ลคร. C- 16 มค 56
ผอ.สวค. 16 มค 56
ผชช. 16 มค. 56
ผอ.กลุ่ม. 16 มค.56
นวค. 16 ม.ค. 56
ผู้พิมพ์

เรื่อง รายงานผลการพิจารณา/ผลการดำเนินการของคณะรัฐมนตรี
กรณีสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติให้คำปรึกษา/ข้อเสนอแนะ/ความเห็นต่อคณะรัฐมนตรี
เรื่อง การบริหารจัดการระบบการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ

.....

ด้วยสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติได้ให้คำปรึกษา/ข้อเสนอแนะ/ความเห็นต่อคณะรัฐมนตรี เรื่อง การบริหารจัดการระบบการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ ซึ่งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง คือ กระทรวงกลาโหม กระทรวงยุติธรรม กระทรวงวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ สำนักงานปลัดสำนักนายกรัฐมนตรี สำนักข่าวกรองแห่งชาติ สำนักงบประมาณ สำนักงานสภาความมั่นคงแห่งชาติ สำนักงานคณะกรรมการกฤษฎีกา สำนักงาน ก.พ. สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) และสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติได้เสนอความเห็น/ผลการพิจารณา/ผลการดำเนินการ ต่อความเห็นของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ดังนี้

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
๑. ด้านเทคโนโลยีการรักษาความปลอดภัยข้อมูลสารสนเทศของประเทศไทย	การบริหารจัดการระบบการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐ ควรใช้ทั้งกลไกทางกฎหมายและกลไกทางการบริหารผนวกเข้าด้วยกันจึงจะสามารถผลักดันให้เกิดมาตรการด้านต่างๆ ตามที่สภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติได้เสนอความเห็นและข้อเสนอแนะไว้ สำหรับกลไกทางกฎหมายนั้น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเห็นว่า ควรเป็นไปตามหลักการของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งตราขึ้นเพื่อรองรับพัฒนาการทางเทคโนโลยีเกี่ยวกับการติดต่อสื่อสารทางอิเล็กทรอนิกส์และการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีเจตนารมณ์เพื่อรองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ภายใต้หลักการพื้นฐานสำคัญสามประการ คือ (๑) หลักความเท่าเทียมกัน (Functional Equivalent Approach) (๒) หลักความเป็นกลางทางเทคโนโลยี (Technology Neutrality) และ (๓) หลักเสรีภาพในการแสดงเจตนา (Party Autonomy) โดยมีขอบเขตใช้บังคับกับธุรกรรมทางอิเล็กทรอนิกส์ซึ่งครอบคลุมทั้งกิจกรรมทั้งในทางแพ่งและพาณิชย์ รวมถึงการดำเนินการของรัฐที่ใช้วิธีการทางอิเล็กทรอนิกส์
๑.๑ พัฒนาเทคโนโลยีของหน่วยงานที่รับผิดชอบด้านการรักษาความปลอดภัยข้อมูลสารสนเทศให้มีเทคโนโลยีทัดเทียมต่างประเทศ โดยเฉพาะประเทศในกลุ่มอาเซียน	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ทั้งนี้ ปัจจุบันพบว่าหน่วยงานของรัฐในประเทศไทยมีความพร้อมด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศอยู่ในระดับที่แตกต่างกันมาก บางหน่วยงานมีความพร้อมในระดับที่ได้รับมาตรฐานสากล เช่น ISO/IEC 27001 เป็นต้น แต่ในบางหน่วยงานยังไม่มีความตระหนัก และยังไม่มีความพร้อมด้านการรักษาความมั่นคงปลอดภัยเลย

/กระทรวง ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เห็นว่าหน่วยงานของรัฐและหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญอย่างยิ่งยวดของประเทศควรมีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศด้วยเทคโนโลยีที่ได้มาตรฐานสากลเป็นอย่างน้อย เพื่อจะได้ทัดเทียมกับต่างประเทศโดยเฉพาะประเทศในกลุ่มอาเซียน อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยสารสนเทศเป็นหน้าที่ของหน่วยงานทุกหน่วยงานและบุคคลทุกคน ปัจจุบันมีการส่งเสริม สนับสนุน และกำกับดูแลให้หน่วยงานและบุคคลมีการรักษาความมั่นคงและปลอดภัยในหลายภาคส่วน เช่น คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงวิทยาศาสตร์และเทคโนโลยี สำนักงานสภาความมั่นคงแห่งชาติ สำนักข่าวกรองแห่งชาติ และสำนักงานตำรวจแห่งชาติ เป็นต้น ทั้งนี้ มีตัวอย่างผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้อง ณ ปัจจุบัน เช่น (๑) สำนักงานตำรวจแห่งชาติได้กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ ดังนี้ - มีการกำหนดสิทธิการเข้าใช้งานข้อมูลตามตำแหน่งหน้าที่ความรับผิดชอบ - มีการจัดเก็บ log ผู้ใช้งานสืบค้นข้อมูลทะเบียนราษฎร์และข้อมูลทะเบียนรถ - ดำเนินการจัดทำระบบรักษาความปลอดภัยระบบสารสนเทศสำนักงานตำรวจแห่งชาติ โดยมุ่งพัฒนาโครงสร้างพื้นฐานรวมทั้งอุปกรณ์และเครื่องมือด้านเทคโนโลยีสารสนเทศเชิงบูรณาการ เพื่อเพิ่มประสิทธิภาพการรักษาความปลอดภัยระบบสารสนเทศหลักและป้องกันการโจมตีจากภายนอก - ใช้เครือข่ายการสื่อสารข้อมูลโทรคมนาคมของสำนักงานตำรวจแห่งชาติผ่านโครงข่าย IP Network ในลักษณะ VPN (Virtual Private Network) จากสำนักงานตำรวจแห่งชาติไปยังหน่วยงานต่างๆ ในสังกัดสำนักงานตำรวจแห่งชาติและส่วนราชการที่เกี่ยวข้อง - มีระบบรักษาความปลอดภัยในการรับส่งข้อมูลแบบเข้ารหัสเพื่อรับส่งข้อมูลระหว่างกันโดยใช้เทคโนโลยีแบบ IPSec - เก็บข้อมูลการเข้าใช้งานคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ - เสนอโครงการจัดหาระบบรักษาความปลอดภัยของศูนย์ประมวลผลสารสนเทศสำรอง ใช้งบประมาณ ๑๒,๐๐๐,๐๐๐ บาท

/(๒) ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
	(๒) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นหน่วยปฏิบัติและเทคนิคด้านการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (e-Transaction) ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการในส่วนที่เกี่ยวข้อง เช่น - งาน ThaiCERT ซึ่งสอดคล้องกับแผนแม่บทไอซีทีของอาเซียน - การผลักดันให้มีการแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Committee) โดยมีนายกรัฐมนตรีเป็นประธานและประกอบไปด้วยผู้แทนของหน่วยราชการต่างๆ ที่เกี่ยวข้อง ๑๔ หน่วยงาน (๓) สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นหน่วยปฏิบัติและเทคนิคด้านการพัฒนารัฐบาลอิเล็กทรอนิกส์ (e-Government) ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการในส่วนที่เกี่ยวข้อง เช่น - จัดตั้งศูนย์ Government Security Operation Center (G-SOC) - จัดทำแผนการประเมินความเสี่ยงทดสอบจุดอ่อนของหน่วยงานภาครัฐ - การสร้างกลุ่ม Cloud Security Alliance Thailand Chapter (CSA Thailand)
๑.๒ พัฒนาระบบการจัดเก็บและสำรองข้อมูล (Backup Data & Restore Data) และให้มีการทดสอบระบบอย่างน้อยปีละ ๑ ครั้ง ให้เป็นมาตรฐานเดียวกันทุกหน่วยงาน	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ปัจจุบันข้อเสนอแนะดังกล่าวได้รับการปฏิบัติและดำเนินการอยู่แล้ว โดยผ่านกลไกของกฎหมายผนวกกับกลไกของการบริหารในการดำเนินการ กล่าวคือ ๑. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ออกประกาศเรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ๒. พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ตราขึ้นเพื่อส่งเสริมให้มีการบริหารจัดการและรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ นอกจากมาตรการทางกฎหมายข้างต้นที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ดำเนินการไปแล้ว กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารยังใช้กลไกทางการบริหารเพื่อดำเนินการในส่วนที่เกี่ยวข้องโดยผ่านทางหน่วยปฏิบัติและเทคนิค ดังนี้ - มอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ดำเนินการเพื่อให้มีแผนในการพัฒนาระบบ National Digital Archive ซึ่งเป็นระบบจัดเก็บข้อมูลขนาดใหญ่ - มอบหมายให้สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ดำเนินการให้มีระบบจัดเก็บข้อมูลและสำรองข้อมูล และมีแผนการทดสอบอย่างน้อยปีละ ๑ ครั้ง สำหรับบริการของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (เฉพาะบริการที่กำหนด)

/นอกจากนี้ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
	นอกจากนี้ สำนักงานตำรวจแห่งชาติยังได้พัฒนาระบบการจัดเก็บและสำรองข้อมูล (Backup Data & Restore Data) ของงานระบบสารสนเทศ ดังนี้ ๑. ดำเนินการ Backup Data ในอุปกรณ์สำรองข้อมูลของศูนย์ข้อมูลกลาง และมีการตรวจสอบการทำงานให้เป็นไปตามระยะเวลาที่กำหนด ๒. ดำเนินการ Backup Data ไปยังศูนย์ประมวลผลสารสนเทศสำรอง เมื่อเกิดภาวะฉุกเฉินสามารถ Restore Data มายังศูนย์ประมวลผลสารสนเทศหลักได้ **ข้อสังเกตเพิ่มเติม** ตลอดระยะเวลาที่ผ่านมานับแต่พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มีผลใช้บังคับ แม้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจะได้พยายามผลักดันให้หน่วยงานของรัฐจัดให้มีระบบสำรองสารสนเทศเพื่อรักษาสภาพพร้อมใช้และกำหนดให้มีการตรวจสอบอย่างสม่ำเสมอ โดยผ่านกลไกทางกฎหมายตามประกาศคณะกรรมการทางธุรกรรมทางอิเล็กทรอนิกส์ แต่ยังขาดกลไกในการส่งเสริมและสนับสนุนด้านเงินงบประมาณ จึงทำให้แต่ละหน่วยงานจัดทำและพัฒนาระบบการจัดเก็บและสำรองข้อมูล (Backup Data & Restore Data) ตามแต่จำนวนเงินงบประมาณที่ได้รับการจัดสรร
๑.๓ ควรมีศูนย์จัดเก็บข้อมูลและสำรองข้อมูลกลาง (Hot site) ที่มีมาตรฐานความปลอดภัยเพื่อจัดเก็บข้อมูล	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ปัจจุบันกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ดำเนินการในส่วนที่เกี่ยวข้องผ่านทางสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งเป็นหน่วยงานทางเทคนิคและผู้ปฏิบัติ เช่น - อยู่ระหว่างการวิเคราะห์ศึกษาการพัฒนาระบบ Backup Site (Hot Site) และ DR Site - อยู่ระหว่างการวิเคราะห์ศึกษาการพัฒนาศูนย์สำรองข้อมูลของหน่วยงานภาครัฐที่มีข้อมูลสำคัญต่อประเทศอย่างยิ่งยวด (Government Critical Infrastructure)

/- สำหรับ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
	- สำหรับสำนักงานตำรวจแห่งชาตินั้น อยู่ระหว่างดำเนินโครงการพัฒนาศูนย์ประมวลผลสารสนเทศสำรอง DR Site ให้สามารถรองรับการทำงานแบบคู่ขนานได้อย่างสมบูรณ์และมีประสิทธิภาพสูงสุด โดยเสนอโครงการพัฒนาประสิทธิภาพศูนย์ประมวลผลสารสนเทศสำรอง (Backup Site) รองรับการทำงานแบบคู่ขนาน ซึ่งโครงการจะครอบคลุมระบบข้อมูลหลักของสำนักงานตำรวจแห่งชาติ ทั้งระบบ POLIS และ CRIMES งบประมาณในการจัดหาวัสดุ ครุภัณฑ์ จำนวน ๑๐๐ ล้านบาท ทั้งนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเห็นว่า หน่วยงานภาครัฐที่มีข้อมูลสำคัญต่อประเทศอย่างยิ่งยวด (Government Critical Infrastructure) ต้องจัดให้มีศูนย์สำรองข้อมูลที่เหมาะสมกับภารกิจให้เกิดขึ้น ก็จะเป็นประโยชน์ต่อการบริหารจัดการระบบสารสนเทศของภาครัฐได้อย่างแท้จริง
๑.๔ ติดตั้งระบบและอุปกรณ์ป้องกัน (Firewall) ให้มีประสิทธิภาพและทันสมัย	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ทั้งนี้ ควรใช้ทั้งกลไกทางกฎหมายและกลไกทางการบริหารผนวกเข้าด้วยกัน จึงจะสามารถผลักดันให้เกิดการติดตั้งระบบและอุปกรณ์ป้องกันให้มีประสิทธิภาพและทันสมัย ปัจจุบันได้รับการปฏิบัติและดำเนินการอยู่แล้ว
๑.๕ ส่งเสริมให้มีการวิจัยและพัฒนาซอฟต์แวร์ ด้านการรักษาความปลอดภัยข้อมูลสารสนเทศของประเทศไทยโดยเฉพาะให้ได้มาตรฐานสากล เพื่อให้ทุกหน่วยงานภาครัฐสามารถนำไปใช้ได้	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ที่ผ่านมากระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนดนโยบายให้การส่งเสริมงานวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ประเทศไทยสามารถพึ่งพาตนเองได้อย่างยั่งยืนเป็นยุทธศาสตร์สำคัญของ (ร่าง) กรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๕๕ – ๒๕๕๙ ซึ่งยังอยู่ในขั้นตอนปรับปรุงให้สมบูรณ์ก่อนนำเสนอให้คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติพิจารณา กระทรวงวิทยาศาสตร์และเทคโนโลยีเห็นด้วยกับที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ดำเนินการในเรื่องการวิจัยและพัฒนาว่าควรสนับสนุนให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยีในการทำวิจัยเรื่องความมั่นคงปลอดภัยของสารสนเทศ เนื่องจากภารกิจหลักของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ คือการวิจัยด้าน IT ซึ่งปัจจุบันได้ดำเนินการอยู่และมีความพร้อมด้านบุคลากร

/๑.๖ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
๑.๖ ปรับปรุงระบบให้สามารถเชื่อมโยงของหน่วยงานภาครัฐได้อย่างสมบูรณ์ในรูปแบบที่เป็นมาตรฐาน และสามารถรองรับการให้บริการแก่ประชาชน	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้มีการดำเนินการที่เกี่ยวข้องกับการเชื่อมโยงของหน่วยงานภาครัฐทั้งในด้านมาตรฐานการแลกเปลี่ยนข้อมูล และการเชื่อมโยงด้านเครือข่าย ได้แก่ โครงการพัฒนากรอบแนวทางมาตรฐานการแลกเปลี่ยนข้อมูลแห่งชาติ (Thailand e-Government Interoperability Framework : TH e-GIF) และโครงการพัฒนาเครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (Government Information Network : GIN) จากสองโครงการดังกล่าว หน่วยงานภาครัฐสามารถปรับปรุงระบบ โดยใช้มาตรฐานการแลกเปลี่ยนข้อมูล TH e-GIF และเชื่อมโยงผ่านเครือข่าย GIN เพื่อรองรับการพัฒนาบริการสำหรับให้บริการแก่ประชาชนได้ นอกจากนี้ ยังมีผลการดำเนินการของ สำนักงานตำรวจแห่งชาติ ดังนี้ ๑. เข้าร่วมโครงการพัฒนาระบบ Government Information Network (GIN) ที่เชื่อมต่อหน่วยงานภาครัฐต่างๆ เพื่อใช้ในการรับส่งข้อมูล ๒. มีการพัฒนาระบบบริการข้อมูลผ่านทางสมาร์ทโฟนและแท็บเล็ตเพื่อให้บริการประชาชน ๓. มีการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างสำนักงานตำรวจแห่งชาติกับหน่วยงานภายนอก ส่วนที่ดำเนินการแล้ว ได้แก่ ๓.๑ กรมการปกครอง ได้แก่ ข้อมูลทะเบียนราษฎร์ ๓.๒ กรมการขนส่งทางบก ได้แก่ ข้อมูลทะเบียนรถยนต์ ส่วนที่อยู่ระหว่างดำเนินการ ได้แก่ ๓.๓ สำนักงานประกันสังคม ๓.๔ กระทรวงสาธารณสุข ๓.๕ กรมการปกครอง (ข้อมูลปืน) ๔. เชื่อมโยงเครือข่ายระหว่างสำนักงานตำรวจแห่งชาติกับสำนักงานทะเบียนราษฎร์ สำนักงานประกันสังคม สำนักการสอบสวนและนิติการ กรมการปกครอง และกรมการขนส่งทางบก

/๒. ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
๒. ด้านข้อกฎหมาย ระเบียบและข้อบังคับ ๒.๑ กำหนดนโยบายให้ ๒ หน่วยงาน คือ สำนักงานรัฐบาลอิเล็กทรอนิกส์ และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) เป็นศูนย์กลางในการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ สนับสนุนงบประมาณ เพิ่มบุคลากรการพัฒนาประสิทธิภาพการดำเนินการ ปรับโครงสร้างการบริหารงานให้เหมาะสมกับภารกิจในด้านการรักษาความปลอดภัยข้อมูลสารสนเทศ โดยให้อยู่ภายใต้การกำกับดูแลอย่างเป็นเอกภาพของคณะกรรมการรักษาความปลอดภัยข้อมูลสารสนเทศแห่งชาติ ซึ่งมีนายกรัฐมนตรีเป็นประธาน	ปัจจุบัน กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีการกำหนดนโยบายเพื่อให้ ๒ หน่วยงาน คือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ให้เป็นศูนย์กลางในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐ โดยสนับสนุนงบประมาณ และเพิ่มบุคลากรเพื่อการพัฒนาประสิทธิภาพการดำเนินการ รวมทั้งการปรับโครงสร้างการบริหารงานให้เหมาะสมกับภารกิจในด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ โดยมีงาน ThaiCERT เพื่อทำหน้าที่เป็นศูนย์กลางในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐ อยู่ในสังกัดสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ทั้งนี้ ได้มีการแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Committee) โดยมีนายกรัฐมนตรีเป็นประธาน เพื่อกำกับดูแลงานของศูนย์กลางในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐอย่างเป็นเอกภาพ นอกจากนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ยังได้ให้ความสำคัญกับการดำเนินงานของ ThaiCERT และสนับสนุนข้อมูลด้านความมั่นคงปลอดภัยให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อกำหนดนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยของการทำธุรกรรมทางอิเล็กทรอนิกส์ในหน่วยงานทั้งภาครัฐและเอกชนอีกทางหนึ่งด้วย สำหรับสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ในส่วนของ Government Security Operation Center (G-SOC) สามารถร่วมมือกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ในส่วนที่เป็น ThaiCERT และหน่วยงานอื่นๆ ที่เกี่ยวข้อง เพื่อประสานงานในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของภาครัฐได้เป็นอย่างดี
๒.๒ ปรับปรุงบทบัญญัติกฎหมาย ระเบียบ ข้อบังคับอื่นใด รวมถึง การตรากฎหมาย ระเบียบข้อบังคับใหม่ ให้มีความสอดคล้องเหมาะสมกับการดำเนินการของศูนย์กลางในการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ โดยให้พิจารณาถึงข้อกฎหมายและอำนาจหน้าที่ในส่วนราชการอื่น พร้อมบทบัญญัติที่เกี่ยวข้องโดยครอบคลุมและรอบคอบ พร้อมคำนึงถึงผลกระทบในมิติต่างๆ ของประเทศโดยละเอียดถี่ถ้วนเช่นกัน ทั้งนี้ อาจจะต้องมีการศึกษาวิจัยถึงความเหมาะสมของการมีศูนย์กลางในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐ และหน่วยงานใดจะเป็นผู้ดำเนินการ จึงมิอาจชี้ชัดได้ในขณะนี้

/๒.๓ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
๒.๓ ออกข้อกำหนด บทบัญญัติ ระเบียบ ข้อบังคับอื่นใด ให้หน่วยงานของรัฐทุกหน่วยงานต้องประสานเชื่อมต่อข้อมูลตามลำดับชั้นความลับของข้อมูลกับศูนย์กลางในการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ โดยให้พิจารณาถึงข้อกฎหมายและอำนาจหน้าที่ในส่วนราชการอื่น พร้อมบทบัญญัติที่เกี่ยวข้องโดยครอบคลุมและรอบคอบ โดยคำนึงถึงผลกระทบในมิติต่างๆ ของประเทศโดยละเอียดถี่ถ้วนเช่นกัน ซึ่งก็ขึ้นอยู่กับข้อเสนอแนะที่ ๒.๒ ว่าจะสมควรให้มีการจัดตั้งศูนย์กลางในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐหรือไม่ หากมีจึงจะสามารถประสานเชื่อมต่อข้อมูลตามลำดับชั้นความลับของข้อมูลกับศูนย์กลางในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐได้ ทั้งนี้ มีหน่วยงานของรัฐที่ได้ดำเนินการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในปัจจุบันจำนวน ๔๒ หน่วยงาน (ข้อมูล ณ ๒๖ ตุลาคม ๒๕๕๕)
๒.๔ มีมาตรการเพิ่มบทลงโทษกับเจ้าหน้าที่ของรัฐที่กระทำความผิด เกี่ยวกับกฎหมายการรักษาข้อมูลสารสนเทศของรัฐ	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ โดยให้พิจารณาถึงข้อกฎหมายและอำนาจหน้าที่ในส่วนราชการอื่น พร้อมบทบัญญัติที่เกี่ยวข้องโดยครอบคลุมและรอบคอบ และคำนึงถึงผลกระทบในมิติต่างๆ ของประเทศโดยละเอียดถี่ถ้วนเช่นกัน ทั้งนี้ หลักการที่จะมีบทลงโทษหรือบทเพิ่มโทษให้แก่เจ้าหน้าที่ของรัฐได้นั้น เจ้าหน้าที่ของรัฐผู้นั้นจะต้องมีหน้าที่ตามกฎหมายเสียก่อน โดยอาจพิจารณาและตราเป็นกฎหมายขึ้นมาเฉพาะก็ได้ อย่างไรก็ตาม มาตรการและบทลงโทษสำหรับเจ้าหน้าที่ของรัฐที่กระทำความผิดเกี่ยวกับกฎหมายการรักษาข้อมูลสารสนเทศของรัฐได้ถูกกำหนดไว้ใน กฎ ระเบียบ ประกาศ ข้อบังคับของแต่ละหน่วยงานอยู่แล้ว รวมทั้งได้มีมาตรการลงโทษทางวินัยของแต่ละองค์กรอยู่แล้ว แต่อาจยังไม่ครอบคลุมเจ้าหน้าที่ของรัฐทุกประเภท จึงควรทบทวนมาตรการเดิมที่มีอยู่แล้วให้ครอบคลุมเจ้าหน้าที่ของรัฐทุกประเภทจะเหมาะสมมากกว่า
๓. ด้านการบริการจัดการระบบการรักษาความปลอดภัยข้อมูลสารสนเทศของรัฐ	การบริหารจัดการระบบการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของรัฐ ถือเป็นหนึ่งกลไกของการบริหารกิจการบ้านเมืองที่ดี ที่สอดคล้องตามนโยบายการบริหารกิจการบ้านเมืองที่ดีของรัฐบาลที่แถลงต่อสภา โดยจัดระบบงานราชการและงานของรัฐอย่างอื่นเพื่อให้การจัดทำและการให้บริการสาธารณะเป็นไปอย่างรวดเร็ว มีประสิทธิภาพ โปร่งใส และตรวจสอบได้โดยคำนึงถึงการมีส่วนร่วมของประชาชน เกิดประสิทธิภาพการบริหารราชการแผ่นดิน

/๓.๑ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
๓.๑ ฝึกอบรมผู้เกี่ยวข้องกับกระบวนการยุติธรรม เช่น พนักงานสอบสวนของสำนักงานตำรวจแห่งชาติ เจ้าหน้าที่พิสูจน์หลักฐานของสถาบันนิติวิทยาศาสตร์ เจ้าหน้าที่สืบสวนของกรมสอบสวนคดีพิเศษ ตลอดจนอัยการและผู้พิพากษา ให้เกิดความรู้ความเข้าใจ เตรียมพร้อมกับกฎหมายการกระทำผิดเกี่ยวกับคอมพิวเตอร์	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ และควรผลักดันให้มีการดำเนินการผ่านคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อย่างไรก็ตามเรื่องการฝึกอบรมจำเป็นต้องฝึกอบรมให้กับเจ้าหน้าที่ทุกระดับ และทุกประเภท มิใช่เฉพาะผู้ที่เกี่ยวข้องกับกระบวนการยุติธรรม เพียงแต่หลักสูตรและความเข้มข้นในแต่ละระดับอาจแตกต่างกันออกไปตามความจำเป็นของแต่ละประเภทเจ้าหน้าที่ ทั้งนี้ มีตัวอย่างผลการดำเนินการของหน่วยงานที่เกี่ยวข้อง ดังนี้ ๑. สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติเป็นผู้ริเริ่มให้มีการจัดฝึกอบรมเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้แก่บุคลากรในกระบวนการยุติธรรม ๒. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยสำนักงานปลัดกระทรวง ได้มีการจัดฝึกอบรมให้แก่ผู้ที่จะได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รวมทั้งได้มีการสร้างความรู้ความเข้าใจให้กับประชาชนทั่วไป นิสิตนักศึกษา นักเรียน และเยาวชนทั่วไปด้วย ๓. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้มีการจัดฝึกอบรมให้บุคลากรในกระบวนการยุติธรรมในหัวข้อที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ในเรื่องการตรวจสอบและวิเคราะห์พยานหลักฐานทางอิเล็กทรอนิกส์บนอุปกรณ์โทรศัพท์เคลื่อนที่
๓.๒ ให้มีนโยบายการเข้าถึงและป้องกันแหล่งข้อมูลสารสนเทศเป็นระดับชั้น	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ อย่างไรก็ตาม การให้มีนโยบายการเข้าถึงและป้องกันแหล่งข้อมูลสารสนเทศเป็นระดับชั้นนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเห็นว่า เป็นไปตามหลักการภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติมแล้ว กล่าวคือ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งเป็นกฎหมายในลำดับรองได้กำหนดให้ทุกหน่วยงานต้องดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของแต่ละหน่วยงาน ซึ่งครอบคลุมการกำหนดให้มีนโยบายการเข้าถึงและป้องกันแหล่งข้อมูลสารสนเทศเป็นระดับชั้นแล้ว

/๓.๓ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
๓.๓ กำหนดให้หน่วยงานของรัฐมีแผนในการบริหารจัดการเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยข้อมูลสารสนเทศเพื่อเตรียมรับกับสถานการณ์ฉุกเฉินด้านความปลอดภัยสารสนเทศที่อาจเกิดขึ้นและส่งผลกระทบต่อการทำงานโดยรวมของหน่วยงานได้	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของ สภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ และควรผลักดันให้มีการดำเนินการผ่านคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยร่วมกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ทั้งนี้ มีตัวอย่างผลการดำเนินการของหน่วยงานที่เกี่ยวข้อง ดังนี้ ๑. สำนักงานตำรวจแห่งชาติ มีการกำหนดแผนและประสานงานกับหน่วยงานที่เกี่ยวข้อง เพื่อเตรียมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้น ๒. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ทำงานสนับสนุนคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งครอบคลุมการกำหนดให้มีนโยบายที่กล่าวถึง ๓. สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) มีแผน มีแนวทาง และการอบรม พร้อมกับการซ้อมแผนสำหรับหน่วยงานที่เข้าร่วมโครงการ Government IT Security Monitoring (GovMon)
๓.๔ พัฒนาระบบการรักษาความปลอดภัยของข้อมูลสารสนเทศของรัฐตามชั้นความลับต้องได้รับการดูแลครอบคลุมในทุกหน่วยงานตามมาตรฐานชั้นความลับและความสำคัญของหน่วยงาน	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ และควรผลักดันให้มีการดำเนินการผ่านคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติร่วมกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ อย่างไรก็ตาม เกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศของรัฐตามชั้นความลับนี้ ปัจจุบันมีระเบียบของราชการที่สามารถใช้บังคับกับกรณีนี้ได้อยู่แล้ว ได้แก่ ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ. ๒๕๒๕ และระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับขอบทางราชการที่สามารถใช้บังคับกับชั้นความลับของข้อมูลทั้งที่เป็นกระดาษและอิเล็กทรอนิกส์
๓.๕ กำหนดแผนยุทธศาสตร์ด้านความปลอดภัยระบบสารสนเทศในระยะยาวให้ชัดเจน เพื่อเป็นแนวทางในการดำเนินการด้านสารสนเทศและการรักษาความปลอดภัยข้อมูลสารสนเทศ ตลอดจนแผนระยะกลางและแผนระยะสั้น เช่น หน่วยงานของรัฐควรมีการจัดทำการประเมินความเสี่ยงระบบสารสนเทศเป็นประจำทุกปี และควรมีการจัดทำแผนฝึกอบรมทุกๆ ๓-๖ เดือน เป็นต้น	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ ทั้งนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานภาครัฐหลักที่มีหน้าที่วางแผน บริหารจัดการ ส่งเสริมสนับสนุน และประสานงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของประเทศร่วมกับหน่วยงานทุกภาคส่วนเพื่อเพิ่มศักยภาพในการแข่งขันของประเทศและเพื่อเกิดการพัฒนาต่อเนื่องอย่างยั่งยืน และให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของประเทศเป็นอย่างมาก ดังที่ได้จัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีนายกรัฐมนตรีเป็นประธาน มีหัวหน้าส่วนราชการที่เกี่ยวข้องร่วมเป็นองค์ประกอบเมื่อต้นปี พ.ศ. ๒๕๕๕ เพื่อจัดทำกรอบนโยบายและแผนแม่บทความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ของประเทศไทย

/ให้สามารถ ...

ความเห็นและข้อเสนอแนะของสภาที่ปรึกษาฯ	ความเห็น/ผลการพิจารณา/ผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับหน่วยงานที่เกี่ยวข้อง
	ให้สามารถปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามไซเบอร์ อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ รวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ซึ่งแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยของระบบสารสนเทศตลอดจนการกำหนดมาตรการในการป้องกันความมั่นคงปลอดภัยข้อมูลสารสนเทศของหน่วยงานนั้นเป็นองค์ประกอบสำคัญของ (ร่าง) กรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๕๕ – ๒๕๕๙ ซึ่งจะเป็นกรอบนโยบายให้หน่วยงานกำหนดแผนแม่บทและแผนปฏิบัติการในระยะยาว/กลาง/สั้นที่สอดคล้องกับกรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย
๓.๖ จัดสรรงบประมาณและเพิ่มจำนวนอัตราบุคลากรที่มีความเชี่ยวชาญด้านเทคโนโลยีระบบสารสนเทศให้เพียงพอต่อความต้องการของหน่วยงาน	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ โดยขอให้รัฐบาลพิจารณาสนับสนุนงบประมาณในสัดส่วนเพิ่มขึ้นและต่อเนื่องในการดำเนินการ พร้อมจัดสรรบุคลากรให้เพียงพอและมีคุณภาพที่ดีและเหมาะสมในภารกิจ และควรผลักดันให้มีการดำเนินการผ่านคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๓.๗ ส่งเสริมการศึกษาด้านเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยของข้อมูลสารสนเทศ โดยบรรจุไว้ในหลักสูตรการศึกษาทุกระดับชั้น	เห็นชอบด้วยและรับในหลักการตามข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ อย่างไรก็ตามผู้ที่จะพิจารณาเกี่ยวกับการบรรจุหลักสูตรการศึกษาด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศไว้ในหลักสูตรการศึกษาทุกระดับชั้นหรือไม่นั้น ควรจะเป็นกระทรวงศึกษาธิการ ส่วนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารอาจทำหน้าที่ในการกำหนดเนื้อหาและรายละเอียดของแต่ละหลักสูตรตามที่กระทรวงศึกษาธิการกำหนด ปัจจุบัน กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) อยู่ระหว่างการร่วมมือกับสมาคม TISA (Thailand Information Security Association) เพื่อจัดทำหลักสูตรเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และแนวทางการรับรองบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศ

คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๑๕ มกราคม ๒๕๕๖ ว่า

๑. รับทราบความเห็นและข้อเสนอแนะของสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ

๒. รับทราบความเห็น ผลการพิจารณา และผลการดำเนินการของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารร่วมกับกระทรวงกลาโหม กระทรวงยุติธรรม กระทรวงวิทยาศาสตร์และเทคโนโลยี กระทรวงศึกษาธิการ สำนักงานปลัดสำนักนายกรัฐมนตรี สำนักข่าวกรองแห่งชาติ สำนักงบประมาณ สำนักงานสภาความมั่นคงแห่งชาติ สำนักงานคณะกรรมการกฤษฎีกา สำนักงาน ก.พ. สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) และสภาที่ปรึกษาเศรษฐกิจและสังคมแห่งชาติ

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๕๖

(นายอำพน กิตติอำพน)
เลขาธิการคณะรัฐมนตรี
17 ม.ค. 2556

รอง ลคร. ..... 16 ม.ค. 56
ผอ.สวค. ..... 16 ม.ค. 56
ผชช. ..... 16 ม.ค. 56
ผอ.กลุ่ม. ..... 16 ม.ค. 56
นวค. ..... 16 ม.ค. 56
ผู้พิมพ์ .....