บันทึกข้อความ

ส่วนราชการ กลุ่มตรวจสอบภายใน (กตน.) โทร. ๔๘๓๔

ที่ นร ๐๑๑๒/ ๑๙๕ **วันที่** ๒๙ มิถุนายน ๒๕๖๕

เรื่อง รายงานผลการตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๔ – พฤษภาคม ๒๕๖๕)

เรียน ปนร.

๑. ประกาศและพระราชบัญญัติที่เกี่ยวข้อง

๑.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่ปรับปรุง (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

๑.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๒. การดำเนินการ

กตน. ได้ตรวจสอบตามแผนการตรวจสอบประจำปีงบประมาณ พ.ศ. ๒๕๖๕ กำหนดไว้ เรื่อง การดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๔ – พฤษภาคม ๒๕๖๕) สรุปผลการตรวจสอบได้ดังนี้

ผลการตรวจสอบ	ข้อเสนอแนะ
๑. นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ๑.๑ การจัดทำนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. เป็นลายลักษณ์อักษร ดังนี้ **(๑) นโยบาย** โดยมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๑) การเข้าถึงหรือการควบคุมการใช้สารสนเทศ ๒) การจัดระบบสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน และแผนเตรียมความพร้อมกรณีฉุกเฉิน และ ๓) การจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ **(๒) ข้อปฏิบัติ** โดยมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๑) การควบคุมการเข้าถึงระบบสารสนเทศ/ระบบเครือข่าย/ระบบปฏิบัติการ ๒) การจัดการเข้าถึงและหน้าที่ความรับผิดชอบของผู้ใช้งาน ๓) การจัดทำระบบสำรองข้อมูลสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และ ๔) การจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	

๑.๒ สปน. ...

ผลการตรวจสอบ	ข้อเสนอแนะ
๑.๒ สปน. ได้มีประกาศสำนักนายกรัฐมนตรี เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์ ของ สปน. ลงวันที่ ๒๐ เมษายน ๒๕๕๕ โดยมีการประกาศฯ ให้ผู้ที่เกี่ยวข้องทราบทางระบบ intranet สปน. และขณะนี้อยู่ระหว่างการทบทวน (ร่าง) แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. เพื่อส่งให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ตรวจสอบ ๑.๓ มีการกำหนดผู้รับผิดชอบตามหน้าที่ของแต่ละบุคคลไว้ในแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๕	- เมื่อสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ตรวจสอบ แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. แล้วเสร็จ ควรมีการประกาศแนวนโยบาย แนวปฏิบัติและเผยแพร่หลายช่องทาง เพื่อให้ผู้ที่เกี่ยวข้องทั้งหมดทราบทั่วกัน เช่น ผ่านทาง website การแจ้งเวียน ฯลฯ เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
๒. การดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ๒.๑ ศทก. ได้มีการเผยแพร่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบ ผ่านทางเว็บไซต์ของ สปน. พร้อมทั้งเผยแพร่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ผ่านไลน์กลุ่ม สปน. ๒.๒ มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้จำนวนไม่น้อยกว่า ๙๐ วัน โดยจัดหาอุปกรณ์จัดเก็บ Log File ใหม่มาทดแทนอุปกรณ์จัดเก็บเดิมที่มีอายุการใช้งานนานกว่า ๑๐ ปี ๒.๓ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลทางภายภาพ พบว่า (๑) มีการใช้ระบบบัตรผ่านเข้า – ออก ห้อง Data Center ให้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องและมีระบบ access control เพื่อควบคุมการเข้า – ออก เฉพาะผู้ที่ถือบัตร และมีระบบการล็อคประตูอัตโนมัติเมื่อประตูปิด (๒) มีการควบคุมเพื่อป้องกันการบุกรุกโจมตีระบบสารสนเทศ โดยติดตั้ง Firewall และมีการซักซ้อมแผนการป้องกันและแก้ไขปัญหาเมื่อเกิดภาวะฉุกเฉิน ปีละ ๑ ครั้ง โดยได้กำหนดแนวทางปฏิบัติไว้ใน	

ผลการตรวจสอบ	ข้อเสนอแนะ
แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ (๓) มีการทำสัญญาจ้างกับบริษัท ไซท์ เพรพพาเรชั่น แมเนจเมนท์ จำกัด เพื่อบำรุงรักษาอุปกรณ์ไฟฟ้าในห้อง Data Center และตรวจสอบการทำงานทุก ๓ เดือน และทำสัญญาจ้าง บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน) เพื่อให้บริการคู่สายสัญญาณวงจรความเร็วสูงเพื่อใช้บริการอินเทอร์เน็ต และบำรุงรักษาซ่อมแซมเครื่องมือ วัสดุและอุปกรณ์ที่ให้บริการทุกชนิด ๒.๔ มีการกำหนดสิทธิการให้บริการระบบเครือข่ายไร้สาย (OPM WiFi) ของ สปน. แบ่งเป็น ๒ ส่วน คือ ๑) ผู้ใช้งานภายใน สปน. และ ๒) ผู้ใช้งานภายนอก สปน. (ผู้มาติดต่อราชการ) โดยกำหนดหลักเกณฑ์และขั้นตอนในการลงทะเบียนผู้ใช้งานตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สปน. ๒.๕ ศทก. ได้ดำเนินการเกี่ยวกับข้อมูลและสารสนเทศต่าง ๆ โดยกำหนดไว้ในนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ดังนี้ (๑) การจัดประเภทของข้อมูลและสารสนเทศ เช่น การกำหนดการเข้าถึงข้อมูลเป็นไปตามลำดับชั้นความลับของข้อมูล (๒) การจัดชั้นความลับของข้อมูลและสารสนเทศ ศทก. ไม่มีการกำหนดชั้นความลับของข้อมูลไว้ หากมีข้อมูลลับจะไม่มีการนำข้อมูลเข้าสู่ระบบสารสนเทศ (๓) การจัดชั้นการเข้าถึงเป็นไปตามลำดับชั้นความลับของข้อมูล เช่น ระบบงานบริหารงานบุคคล (๔) การกำหนดเวลาในการเข้าถึง ศทก. ได้กำหนดเวลาการเข้าถึงข้อมูลบางระบบที่มีความจำเป็น เช่น การเข้าใช้ประโยชน์ข้อมูลทะเบียนประวัติราษฎร (๕) การกำหนดช่องทางในการเข้าถึง ศทก. ได้กำหนดช่องทางให้ผู้ใช้เข้าถึงระบบได้ตามความเหมาะสม โดยแบ่งเป็น ๒ ช่องทาง ได้แก่ ๑) ระบบสำหรับเจ้าหน้าที่ สปน. สามารถเข้าถึงระบบด้วย	

ช่องทาง...

ผลการตรวจสอบ	ข้อเสนอแนะ
ช่องทาง Intranet และ ๒) ระบบสำหรับบุคคลทั่วไปสามารถเข้าถึงระบบด้วยช่องทาง Internet ๒.๖ การควบคุมและจำกัดสิทธิผู้ใช้ระบบ พบว่ามีการกำหนดให้ลงทะเบียนผู้ใช้งานเพื่ออนุญาตและเพิกถอนสิทธิ โดยมีระบบกำหนดสิทธิในการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่ โดยหน่วยงานต้นสังกัดต้องทำหนังสือถึง ศทก. เป็นลายลักษณ์อักษร มอบหมายให้ผู้ใช้งานเข้าถึงระบบเฉพาะของหน่วยงานตลอดจนการเพิ่มเติม/ยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบของเจ้าหน้าที่ที่ได้รับมอบหมาย โดย ศทก. จะมีหนังสือแจ้งหน่วยงานต้นสังกัด พร้อมแนบรหัสผ่านรายบุคคลด้วยการจัดใส่ซองปิดผนึกและเซ็นชื่อกำกับบริเวณผนึก และมีการกำหนดการเพิกถอนสิทธิ และเงื่อนไขให้ผู้ใช้ระบบต้องเก็บรักษารหัสผ่านของตนเองและของกลุ่มงานไว้เป็นความลับ และเนื่องจากระบบสารสนเทศบางระบบมีความจำเป็นต้องใช้ User ร่วม เพื่อเข้าถึงข้อมูลของแต่ละกลุ่มงานหรือหน่วยงานด้วยUser เดียวกันจะไม่มีการจัดเก็บข้อมูลเฉพาะบุคคล และผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการที่ได้รับสิทธิเท่านั้น ในกรณีที่ผู้ใช้งานจากภายนอกเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน จะมีกระบวนการในการยืนยันตัวบุคคลก่อนอนุญาตให้เข้าระบบ และกำหนดให้มีการทบทวนสิทธิเข้าถึงระบบสารสนเทศของผู้ใช้งานทุก ๑ ปี และมีการทบทวนสิทธิอย่างต่อเนื่อง โดย ศทก. ได้มีการเผยแพร่หลักเกณฑ์ระบบสารสนเทศทางเว็บไซต์ภายใน สปน. (Intranet) และหากมีการพัฒนาระบบสารสนเทศใหม่จะมีการแจ้งเวียนให้ผู้ใช้ระบบทราบต่อไป ทั้งนี้ ศทก. ยังไม่มีการให้ความรู้ ความเข้าใจแก่ผู้ใช้งานถึงภัยและผลกระทบจากการใช้งานระบบโดยไม่ระมัดระวังและรู้เท่าไม่ถึงการณ์ ๒.๗ การเตรียมความพร้อมกรณีฉุกเฉิน พบว่า ศทก. มี Site สำรอง Co – Location ในกรณีที่ Site หลักไม่ทำงาน และมีการกำหนดเป็นแผนระยะสั้นไว้ในแผนบริหารความเสี่ยง ปีงบประมาณ พ.ศ. ๒๕๖๕ และ ศทก.	- ควรมีการแนะนำให้กับผู้ใช้งานเกี่ยวกับการใช้ชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่โดยให้มีความระมัดระวัง เพื่อให้ผู้ใช้งานปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

ได้มีการ...

ผลการตรวจสอบ	ข้อเสนอแนะ
ได้มีการทดสอบระบบให้อยู่ในสภาพพร้อมในการใช้งาน ประกอบด้วย (๑) ระบบสารสนเทศ ได้มีการทดสอบการใช้งานเป็นประจำทุก ๒ เดือน โดยมีการทดสอบครั้งสุดท้าย เมื่อวันที่ ๑๐ - ๑๒ พฤษภาคม ๒๕๖๕ (๒) ระบบสำรองข้อมูลระบบสารสนเทศของ สปน. ได้มีการทดสอบครั้งสุดท้าย เมื่อวันที่ ๗ พฤษภาคม ๒๕๖๕ (๓) แผนฉุกเฉิน ได้มีการซักซ้อมการปฏิบัติตามแผนบริหารความเสี่ยงกรณีเกิดเหตุการณ์ชุมนุมทางการเมือง (ปิดล้อมทำเนียบรัฐบาล) เมื่อวันที่ ๒๓ กันยายน ๒๕๖๔	
๓. การดำเนินการตามแผนงาน โครงการ และงบประมาณในการจัดหาและพัฒนาระบบงานสารสนเทศ ศทก. ได้รับจัดสรรงบประมาณเพื่อจัดหาและพัฒนาระบบสารสนเทศ ของ สปน. จำนวน ๒๒,๒๕๒,๗๒๗ บาท พบว่า ณ วันที่ ๓๑ พฤษภาคม ๒๕๖๕ มีผลการเบิกจ่ายทั้งสิ้น ๑๐,๖๙๑,๑๕๐ บาท คิดเป็นร้อยละ ๔๘.๐๔ สรุปได้ดังนี้ ๓.๑ การบำรุงรักษาระบบและอุปกรณ์ระบบสารสนเทศ จำนวน ๕ รายการ รวมเป็นเงิน ๑๔,๘๗๗,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๖,๕๐๗,๒๕๐ บาท ๓.๒ การจัดหาบริการคู่สายสัญญาณวงจรความเร็วสูงเพื่อใช้บริการอินเทอร์เน็ตและบริการระบบประชุมทางไกลผ่านอินเทอร์เน็ต สปน. จำนวน ๒ รายการ รวมเป็นเงิน ๗,๐๕๘,๙๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๔,๑๘๓,๙๐๐ บาท ๓.๓ การจัดหาครุภัณฑ์คอมพิวเตอร์ทดแทนของ สปน. จำนวน ๓๑๖,๘๒๗ บาท ขณะนี้คณะกรรมการตรวจรับพัสดุอยู่ระหว่างการตรวจรับ ๓.๔ เนื่องจากการจัดหาครุภัณฑ์คอมพิวเตอร์ทดแทนของ สปน. มีงบประมาณเหลือจ่ายจากการประหยัดได้จำนวน ๑๙๐,๖๗๓ บาท ศทก. จึงมีแผนจะดำเนินการขออนุมัติโอนเปลี่ยนแปลงรายการงบประมาณรายจ่ายเพื่อจัดหาครุภัณฑ์คอมพิวเตอร์เพิ่มเติมต่อไป	- ควรเร่งดำเนินการขออนุมัติโอนเปลี่ยนแปลงรายการงบประมาณรายจ่าย ในการจัดหาครุภัณฑ์คอมพิวเตอร์เพิ่มเติม เพื่อให้สามารถดำเนินการได้ทันภายในปีงบประมาณ พ.ศ. ๒๕๖๕

๓. ข้อเสนอ

จึงเรียนมาเพื่อโปรดทราบรายงานผลการตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๔ – พฤษภาคม ๒๕๖๕) เพื่อ กตน. จะได้แจ้งให้ ศทก. ทราบและดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางสายพิน สมบัติทอง)
ผอ.กตน.

- ทราบ
- ศทก.สปน. ดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นายธีรภัทร ประยูรสิทธิ)
ปลัดสำนักนายกรัฐมนตรี
๓๐ มิ.ย. ๖๕

รหัสรายงานการตรวจสอบที่ ๑๗/๒๕๖๕

สำนักงานปลัดสำนักนายกรัฐมนตรี
กลุ่มตรวจสอบภายใน

รายงานผลการตรวจสอบ

หน่วยรับตรวจ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทก.) สำนักงานปลัดสำนักนายกรัฐมนตรี (สปน.)

เรื่องที่ตรวจสอบ การดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของ ศทก. สปน.

วัตถุประสงค์ของการตรวจสอบ

๑. เพื่อตรวจสอบการควบคุมและการปฏิบัติงานด้านการรักษาความปลอดภัยระบบสารสนเทศ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่ปรับปรุง (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

๒. เพื่อให้ทราบว่าการจัดหาและพัฒนาระบบงานสารสนเทศมีการดำเนินงานตามแผนการปฏิบัติงานและบรรลุตามวัตถุประสงค์

๓. เพื่อทราบปัญหาอุปสรรคในการปฏิบัติงาน และให้ข้อคิดเห็นและข้อเสนอแนะเพื่อการปรับปรุงแก้ไขการปฏิบัติงานให้แก่หน่วยรับตรวจและผู้ที่เกี่ยวข้อง

ขอบเขตการตรวจสอบ

๑. ดำเนินการสอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติงานด้านการรักษาความปลอดภัยระบบสารสนเทศ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่ปรับปรุง (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ ที่หน่วยงานใช้อยู่ในปัจจุบัน

๒. สุ่มสอบทานการปฏิบัติตามนโยบายและข้อปฏิบัติเพื่อให้เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๓. ตรวจสอบการดำเนินการตามแผนงาน โครงการและงบประมาณในการจัดหาและพัฒนาระบบงานสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ (เดือนตุลาคม ๒๕๖๔ – พฤษภาคม ๒๕๖๕)

ระยะเวลาการตรวจสอบ วันที่ ๓ พฤษภาคม, ๖ - ๙, ๑๓ - ๑๗, ๒๐ - ๒๑ มิถุนายน ๒๕๖๕

วิธีการตรวจสอบ

๑. สอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติงานเพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่ปรับปรุง (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

๒. สอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการปฏิบัติตามนโยบายและข้อปฏิบัติ เพื่อให้เป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๓. ตรวจสอบผลการดำเนินการตามแผนงาน โครงการ และงบประมาณในการจัดหาและพัฒนาระบบงานสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ (เดือนตุลาคม ๒๕๖๔ – พฤษภาคม ๒๕๖๕)

๔. สอบถามเจ้าหน้าที่ผู้รับผิดชอบและผู้ที่เกี่ยวข้อง

สรุปผลการตรวจสอบ

กตน. ได้ตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๔ – พฤษภาคม ๒๕๖๕) สรุปได้ดังนี้

๑. การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ผลการตรวจสอบ	ข้อเสนอแนะ
๑. นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ๑.๑ การจัดทำนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. เป็นลายลักษณ์อักษร ดังนี้ **(๑) นโยบาย** โดยมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๑) การเข้าถึงหรือการควบคุมการใช้สารสนเทศ ๒) การจัดระบบสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน และแผนเตรียมความพร้อมกรณีฉุกเฉิน และ ๓) การจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ **(๒) ข้อปฏิบัติ** โดยมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๑) การควบคุมการเข้าถึงระบบสารสนเทศ/ระบบเครือข่าย/ระบบปฏิบัติการ ๒) การจัดการเข้าถึงและหน้าที่ความรับผิดชอบของผู้ใช้งาน ๓) การจัดทำระบบสำรองข้อมูลสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และ ๔) การจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ๑.๒ สปน. ได้มีประกาศสำนักนายกรัฐมนตรี เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์ ของ สปน. ลงวันที่ ๒๐ เมษายน ๒๕๕๕ โดยมีการประกาศฯ ให้ผู้ที่เกี่ยวข้องทราบทางระบบ intranet สปน. และขณะนี้อยู่ระหว่างการทบทวน (ร่าง) แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. เพื่อส่งให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ตรวจสอบ ๑.๓ มีการกำหนดผู้รับผิดชอบตามหน้าที่ของแต่ละบุคคลไว้ในแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๕	- เมื่อสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ตรวจสอบ แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. แล้วเสร็จ ควรมีการประกาศแนวนโยบายแนวปฏิบัติและเผยแพร่หลายช่องทางเพื่อให้ผู้ที่เกี่ยวข้องทั้งหมดทราบทั่วกัน เช่น ผ่านทาง website การแจ้งเวียน ฯลฯ เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ผลการตรวจสอบ	ข้อเสนอแนะ
๒. การดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ๒.๑ ศทก. ได้มีการเผยแพร่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบ ผ่านทางเว็บไซต์ของ สปน. พร้อมทั้งเผยแพร่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ผ่านไลน์กลุ่ม สปน. ๒.๒ มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้จำนวนไม่น้อยกว่า ๙๐ วัน โดยจัดหาอุปกรณ์จัดเก็บ Log File ใหม่มาทดแทนอุปกรณ์จัดเก็บเดิมที่มีอายุการใช้งานนานกว่า ๑๐ ปี ๒.๓ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลทางภายภาพ พบว่า (๑) มีการใช้ระบบบัตรผ่านเข้า – ออกห้อง Data Center ให้เฉพาะเจ้าหน้าที่ที่เกี่ยวข้องและมีระบบ access control เพื่อควบคุมการเข้า – ออกเฉพาะผู้ที่ถือบัตร และมีระบบการล็อคประตูอัตโนมัติเมื่อประตูปิด (๒) มีการควบคุมเพื่อป้องกันการบุกรุกโจมตีระบบสารสนเทศ โดยติดตั้ง Firewall และมีการซักซ้อมแผนการป้องกันและแก้ไขปัญหาเมื่อเกิดภาวะฉุกเฉิน ปีละ ๑ ครั้ง โดยได้กำหนดแนวทางปฏิบัติไว้ในแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ (๓) มีการทำสัญญาจ้างกับบริษัท ไซท์เพรพพาเรชั่น แมเนจเมนท์ จำกัด เพื่อบำรุงรักษาอุปกรณ์ไฟฟ้าในห้อง Data Center และตรวจสอบการทำงานทุก ๓ เดือน และทำสัญญาจ้าง บริษัท ซีเอสล็อกซอินโฟ จำกัด (มหาชน) เพื่อให้บริการคู่สายสัญญาณวงจรความเร็วสูงเพื่อใช้บริการอินเทอร์เน็ตและบำรุงรักษาซ่อมแซมเครื่องมือ วัสดุและอุปกรณ์ที่ให้บริการทุกชนิด ๒.๔ มีการกำหนดสิทธิการให้บริการระบบเครือข่ายไร้สาย (OPM WiFi) ของ สปน. แบ่งเป็น ๒ ส่วน คือ ๑) ผู้ใช้งานภายใน สปน. และ ๒) ผู้ใช้งานภายนอก สปน. (ผู้มาติดต่อราชการ) โดยกำหนด	

ผลการตรวจสอบ	ข้อเสนอแนะ
หลักเกณฑ์และขั้นตอนในการลงทะเบียนผู้ใช้งานตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของ สปน. ๒.๕ ศทก. ได้ดำเนินการเกี่ยวกับข้อมูลและสารสนเทศต่าง ๆ โดยกำหนดไว้ในนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ดังนี้ (๑) การจัดประเภทของข้อมูลและสารสนเทศ เช่น การกำหนดการเข้าถึงข้อมูลเป็นไปตามลำดับชั้นความลับของข้อมูล (๒) การจัดชั้นความลับของข้อมูลและสารสนเทศ ศทก. ไม่มีการกำหนดชั้นความลับของข้อมูลไว้ หากมีข้อมูลลับจะไม่มีการนำข้อมูลเข้าสู่ระบบสารสนเทศ (๓) การจัดชั้นการเข้าถึงเป็นไปตามลำดับชั้นความลับของข้อมูล เช่น ระบบงานบริหารงานบุคคล (๔) การกำหนดเวลาในการเข้าถึง ศทก. ได้กำหนดเวลาการเข้าถึงข้อมูลบางระบบที่มีความจำเป็น เช่น การเข้าใช้ประโยชน์ข้อมูลทะเบียนประวัติราษฎร (๕) การกำหนดช่องทางในการเข้าถึง ศทก. ได้กำหนดช่องทางให้ผู้ใช้เข้าถึงระบบได้ตามความเหมาะสม โดยแบ่งเป็น ๒ ช่องทาง ได้แก่ ๑) ระบบสำหรับเจ้าหน้าที่ สปน. สามารถเข้าถึงระบบด้วยช่องทาง Intranet และ ๒) ระบบสำหรับบุคคลทั่วไป สามารถเข้าถึงระบบด้วยช่องทาง Internet	
๒.๖ การควบคุมและจำกัดสิทธิผู้ใช้ระบบ พบว่ามีการกำหนดให้ลงทะเบียนผู้ใช้งานเพื่ออนุญาตและเพิกถอนสิทธิ โดยมีระบบกำหนดสิทธิในการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่ โดยหน่วยงานต้นสังกัดต้องทำหนังสือถึง ศทก. เป็นลายลักษณ์อักษร มอบหมายให้ผู้ใช้งานเข้าถึงระบบเฉพาะของหน่วยงานตลอดจนการเพิ่มเติม/ยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบของเจ้าหน้าที่ที่ได้รับมอบหมาย โดย ศทก. จะมีหนังสือแจ้งหน่วยงานต้นสังกัด พร้อมแนบรหัสผ่านรายบุคคลด้วยการจัดใส่ซองปิดผนึกและเซ็นชื่อกำกับบริเวณผนึก และมีการ	- ควรมีการแนะนำให้กับผู้ใช้งานเกี่ยวกับการใช้ชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่ โดยให้มีความระมัดระวัง เพื่อให้ผู้ใช้งานปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

ผลการตรวจสอบ	ข้อเสนอแนะ
กำหนดการเพิกถอนสิทธิ และเงื่อนไขให้ผู้ใช้ระบบต้องเก็บรักษารหัสผ่านของตนเองและของกลุ่มงานไว้เป็นความลับ และเนื่องจากระบบสารสนเทศบางระบบมีความจำเป็นต้องใช้ User ร่วม เพื่อเข้าถึงข้อมูลของแต่ละกลุ่มงานหรือหน่วยงานด้วย User เดียวกันจะไม่มีการจัดเก็บข้อมูลเฉพาะบุคคล และผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการที่ได้รับสิทธิเท่านั้น ในกรณีที่ผู้ใช้งานจากภายนอกเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน จะมีกระบวนการในการยืนยันตัวบุคคลก่อนอนุญาตให้เข้าระบบ และกำหนดให้มีการทบทวนสิทธิเข้าถึงระบบสารสนเทศของผู้ใช้งานทุก ๑ ปี และมีการทบทวนสิทธิอย่างต่อเนื่อง โดย ศทก. ได้มีการเผยแพร่หลักเกณฑ์ระบบสารสนเทศ ทางเว็บไซต์ภายใน สปน. (Intranet) และหากมีการพัฒนาระบบสารสนเทศใหม่จะมีการแจ้งเวียนให้ผู้ใช้ระบบทราบต่อไป ทั้งนี้ ศทก. ยังไม่มีการให้ความรู้ ความเข้าใจแก่ผู้ใช้งานถึงภัยและผลกระทบจากการใช้งานระบบโดยไม่ระมัดระวังและรู้เท่าไม่ถึงการณ์ ๒.๗ การเตรียมความพร้อมกรณีฉุกเฉิน พบว่า ศทก. มี Site สำรอง Co – Location ในกรณีที่ Site หลักไม่ทำงาน และมีการกำหนดเป็นแผนระยะสั้นไว้ในแผนบริหารความเสี่ยง ปีงบประมาณ พ.ศ. ๒๕๖๕ และ ศทก. ได้มีการทดสอบระบบให้อยู่ในสภาพพร้อมในการใช้งาน ประกอบด้วย (๑) ระบบสารสนเทศ ได้มีการทดสอบการใช้งานเป็นประจำทุก ๒ เดือน โดยมีการทดสอบครั้งสุดท้าย เมื่อวันที่ ๑๐ - ๑๒ พฤษภาคม ๒๕๖๕ (๒) ระบบสำรองข้อมูลระบบสารสนเทศของ สปน. ได้มีการทดสอบครั้งสุดท้าย เมื่อวันที่ ๗ พฤษภาคม ๒๕๖๕ (๓) แผนฉุกเฉิน ได้มีการซักซ้อมการปฏิบัติตามแผนบริหารความเสี่ยงกรณีเกิดเหตุการณ์ชุมนุมทางการเมือง (ปิดล้อมทำเนียบรัฐบาล) เมื่อวันที่ ๒๓ กันยายน ๒๕๖๔	

ผลการตรวจสอบ	ข้อเสนอแนะ
๓. การดำเนินการตามแผนงาน/โครงการและงบประมาณในการจัดหาและพัฒนาระบบสารสนเทศ ศทก. ได้รับจัดสรรงบประมาณเพื่อจัดหาและพัฒนาระบบสารสนเทศ ของ สปน. จำนวน ๒๒,๒๕๒,๗๒๗ บาท พบว่า ณ วันที่ ๓๑ พฤษภาคม ๒๕๖๕ มีผลการเบิกจ่ายทั้งสิ้น ๑๐,๖๙๑,๑๕๐ บาท คิดเป็นร้อยละ ๔๘.๐๔ สรุปได้ดังนี้ ๓.๑ การบำรุงรักษาระบบและอุปกรณ์ระบบสารสนเทศ จำนวน ๕ รายการ รวมเป็นเงิน ๑๔,๘๗๗,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๖,๕๐๗,๒๕๐ บาท ๓.๒ การจัดหาบริการคู่สายสัญญาณวงจรความเร็วสูงเพื่อใช้บริการอินเทอร์เน็ตและบริการระบบประชุมทางไกลผ่านอินเทอร์เน็ต สปน. จำนวน ๒ รายการ รวมเป็นเงิน ๗,๐๕๘,๙๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๔,๑๘๓,๙๐๐ บาท ๓.๓ การจัดหาครุภัณฑ์คอมพิวเตอร์ทดแทนของ สปน. จำนวน ๓๑๖,๘๒๗ บาท ขณะนี้คณะกรรมการตรวจรับพัสดุอยู่ระหว่างการตรวจรับ ๓.๔ เนื่องจากการจัดหาครุภัณฑ์คอมพิวเตอร์ทดแทนของ สปน. มีงบประมาณเหลือจ่ายจากการประหยัดได้ จำนวน ๑๙๐,๖๗๓ บาท ศทก. จึงมีแผนจะดำเนินการขออนุมัติโอนเปลี่ยนแปลงรายการงบประมาณรายจ่าย เพื่อจัดหาครุภัณฑ์คอมพิวเตอร์เพิ่มเติมต่อไป	- ควรเร่งดำเนินการขออนุมัติโอนเปลี่ยนแปลงรายการงบประมาณรายจ่าย ในการจัดหาครุภัณฑ์คอมพิวเตอร์เพิ่มเติม เพื่อให้สามารถดำเนินการได้ทันภายในปีงบประมาณ พ.ศ. ๒๕๖๕

๒. การติดตามผลการดำเนินการตามข้อเสนอแนะของ กตน. ในปีที่ผ่านมา

ข้อคิดเห็นและข้อเสนอแนะของ กตน. ในปีที่ผ่านมา	ผลการดำเนินงานของ ศทก.		หมายเหตุ
	ดำเนินการเรียบร้อยแล้ว	ยังไม่ได้ดำเนินการ	
๑. นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ๑.๑ ควรมีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ให้เป็นปัจจุบันอยู่เสมอ		✓	- อยู่ระหว่างการทบทวน (ร่าง) แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัย

ข้อคิดเห็นและข้อเสนอแนะของ กตน. ในปีที่ผ่านมา	ผลการดำเนินงานของ ศทก.		หมายเหตุ
	ดำเนินการเรียบร้อยแล้ว	ยังไม่ได้ดำเนินการ	
๑.๒ ควรมีการประกาศนโยบายและข้อปฏิบัติให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์		✓	ด้านเทคโนโลยีสารสนเทศ สปน. เพื่อส่งให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ตรวจสอบ
๑.๓ ควรมีการกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติให้ชัดเจน เช่น มีคำสั่งหรือหนังสือมอบหมายสั่งการโดยระบุบุคคลผู้รับผิดชอบให้ชัดเจน		✓	
๒. การดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์			
๒.๑ ควรมีคำสั่งหรือหนังสือมอบหมายสั่งการโดยระบุบุคคลผู้รับผิดชอบการเข้า – ออกในพื้นที่เฉพาะให้ชัดเจน	✓		- มีการกำหนดผู้รับผิดชอบตามหน้าที่ของแต่ละบุคคลอย่างชัดเจน ไว้ในแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประจำปีงบประมาณ พ.ศ. ๒๕๖๕
๒.๒ ควรมีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงานเพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบทั่วกัน	✓		
๒.๓ ควรมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	✓		
๓. การดำเนินการตามแผนงาน โครงการ และงบประมาณในการจัดหาและพัฒนาระบบงานสารสนเทศ			
- ควรเร่งดำเนินการปรับปรุงข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้สามารถดำเนินการได้ทันภายในปีงบประมาณ พ.ศ. ๒๕๖๔	✓		- ดำเนินการแล้วเสร็จเมื่อวันที่ ๒๔ ธันวาคม ๒๕๖๔

ผู้ตรวจสอบ
(นางสกาวรัตน์ ทองเทพ)
นวก.ตน.ชพ.
๒๘ มิ.ย. ๒๕๖๕

ผู้กำกับดูแลการตรวจสอบ
(นางสายพิน สมบัติทอง)
ผอ.กตน.
มิ.ย. ๒๕๖๕