บันทึกข้อความ

ส่วนราชการ กลุ่มตรวจสอบภายใน (กตน.) โทร. ๔๘๓๔

ที่ นร ๐๑๑๒/ ๒๒๔ **วันที่** ๗ กรกฎาคม ๒๕๖๔

เรื่อง รายงานผลการตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๓ – พฤษภาคม ๒๕๖๔)

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. ๒๕๖๔ กำหนดไว้ เรื่อง การดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๓ – พฤษภาคม ๒๕๖๔) สรุปผลการตรวจสอบได้ดังนี้

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

ทั้งนี้...

ผลการตรวจสอบ	ข้อเสนอแนะ
๑.๒ สปน. ได้มีประกาศสำนักนายกรัฐมนตรี เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายคุ้มครองข้อมูลส่วนบุคคล ของเว็บไซต์ ของ สปน. ลงวันที่ ๒๐ เม.ย. ๒๕๕๕ อย่างไรก็ดี พบว่า ไม่มีประกาศฯ ให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ ๑.๓ การกำหนดผู้รับผิดชอบเป็นกลุ่มงาน แต่ยังไม่ได้มีการระบุผู้รับผิดชอบในแต่ละด้านเป็นรายบุคคล เช่น (๑) กลุ่มงานบริหารเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบด้านระบบเครือข่ายและการซ่อมบำรุง และ (๒) กลุ่มงานบริหารระบบฐานข้อมูลสารสนเทศ เป็นผู้รับผิดชอบด้านระบบสารสนเทศของ สปน. เป็นต้น	- ควรมีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ให้เป็นปัจจุบันอยู่เสมอ - ควรมีการประกาศนโยบายและข้อปฏิบัติให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ - ควรมีการกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติให้ชัดเจน เช่น มีคำสั่งหรือหนังสือมอบหมายสั่งการโดยระบุบุคคลผู้รับผิดชอบให้ชัดเจน
๒. การดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ๒.๑ การควบคุมความปลอดภัยทางกายภาพของ ศูนย์สารสนเทศ ห้องเก็บสารสนเทศและห้องทำงาน ของ ศทก. พบว่า (๑) มีการปิดล็อกเมื่อไม่มีการใช้งาน และจัดเก็บอุปกรณ์ ครุภัณฑ์ ในตู้ที่มีการควบคุมกุญแจ พร้อมทั้งมีทะเบียนคุมการเบิกจ่าย (๒) มีการควบคุมการเข้า – ออกในพื้นที่เฉพาะโดยมอบหมายเจ้าหน้าที่กลุ่มงานตามภารกิจงานในแต่ละด้านที่รับผิดชอบ ซึ่งยังไม่มีคำสั่งหรือการมอบหมายสั่งการเพื่อระบุตัวบุคคลแต่อย่างใด (๓) มีการควบคุมเพื่อป้องกันการบุกรุกโจมตีโดยติดตั้ง Firewall และมีการซักซ้อมแผนฉุกเฉินกรณีไฟไหม้ ปีละ ๑ ครั้ง (๔) มีการทำสัญญาจ้างกับบริษัท ไซท์ เพรพพาเรชั่น แมเนจเมนท์ จำกัด เพื่อบำรุงรักษาอุปกรณ์ไฟฟ้าในห้อง Data Center และตรวจสอบการทำงานทุก ๓ เดือน และทำสัญญาจ้าง บริษัท ซีเอสล็อกซอินโฟ จำกัด (มหาชน) เพื่อให้บริการคู่สายสัญญาณวงจรความเร็วสูงเพื่อใช้บริการอินเทอร์เน็ตและบำรุงรักษาซ่อมแซมเครื่องมือ วัสดุและอุปกรณ์ที่ให้บริการทุกชนิด	- ควรมีคำสั่งหรือหนังสือมอบหมายสั่งการโดยระบุบุคคลผู้รับผิดชอบการเข้า – ออกในพื้นที่เฉพาะให้ชัดเจน - ควรมีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงานเพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบทั่วกัน

ทั้งนี้...

ผลการตรวจสอบ	ข้อเสนอแนะ
ทั้งนี้ ศทก. ยังไม่มีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบ ๒.๒ การควบคุมด้านข้อมูลและสารสนเทศ ศทก. พบว่า มีการกำหนดสิทธิการเข้าถึงให้กับอุปกรณ์คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ ในการใช้บริการระบบเครือข่ายไร้สาย (OPM WiFi) ของ สปน. และมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้จำนวนไม่น้อยกว่า ๙๐ วัน ทั้งนี้ ศทก. อยู่ระหว่างดำเนินการจัดซื้ออุปกรณ์จัดเก็บ Log File มาทดแทน เนื่องจากอุปกรณ์ที่ใช้อยู่ปัจจุบันมีอายุการใช้งานมากกว่า ๑๐ ปี และได้ดำเนินการเกี่ยวกับข้อมูลและสารสนเทศโดยกำหนดไว้ในนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ดังนี้ (๑) การจัดประเภทของข้อมูล เช่น ข้อมูลภายนอกสามารถเปิดเผยได้ ในส่วนข้อมูลภายในเป็นไปตามลำดับชั้นความลับของข้อมูล (๒) การจัดชั้นความลับของข้อมูล ศทก. ไม่มีการกำหนดชั้นความลับของข้อมูลไว้ ในส่วนของข้อมูลลับจะไม่มีการนำข้อมูลเข้าสู่ระบบสารสนเทศ (๓) การจัดชั้นการเข้าถึงเป็นไปตามลำดับชั้นความลับของข้อมูล เช่น ระบบงานบริหารงานบุคคล (๔) การกำหนดเวลาในการเข้าถึง ศทก. ได้กำหนดเวลาการเข้าถึงข้อมูลบางระบบที่มีความจำเป็น เช่น การเข้าใช้ประโยชน์ข้อมูลทะเบียนประวัติราษฎร (๕) การกำหนดช่องทางในการเข้าถึง ศทก. ได้กำหนดช่องทางให้ผู้ใช้เข้าถึงระบบได้ตามความเหมาะสม โดยแบ่งเป็น ๒ ช่องทาง ได้แก่ ๑) ระบบสำหรับเจ้าหน้าที่ สปน. ๒) ระบบสำหรับบุคคลทั่วไป ๒.๓ การควบคุมและจำกัดสิทธิผู้ใช้ระบบ พบว่า มีการกำหนดสิทธิในการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่	

โดยหน่วยงาน...

ผลการตรวจสอบ	ข้อเสนอแนะ
โดยหน่วยงานต้นสังกัดต้องทำหนังสือถึง ศทก. เป็นลายลักษณ์อักษร และมอบหมายให้ผู้ใช้ระบบเข้าถึงระบบเฉพาะของหน่วยงาน ตลอดจนการเพิ่มเติม/ยกเลิกสิทธิการเข้าใช้ระบบงานของเจ้าหน้าที่ที่ได้รับมอบหมาย โดย ศทก. จะมีหนังสือแจ้งหน่วยงานต้นสังกัด พร้อมแนบรหัสผ่านรายบุคคลด้วยการจัดใส่ซองปิดผนึกและเซ็นชื่อกำกับบริเวณผนึก และมีการกำหนดการเพิกถอนสิทธิและเงื่อนไขให้ผู้ใช้ระบบต้องเก็บรักษารหัสผ่านของตนเองและของกลุ่มงานไว้เป็นความลับ และเนื่องจากระบบสารสนเทศบางระบบมีความจำเป็นต้องใช้ User ร่วม เพื่อเข้าถึงข้อมูลของแต่ละกลุ่มงานหรือหน่วยงานด้วย User เดียวกัน จะไม่มีการจัดเก็บข้อมูลเฉพาะบุคคล และผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการที่ได้รับสิทธิเท่านั้น ในกรณีที่ผู้ใช้งานจากภายนอกเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน จะมีกระบวนการในการยืนยันตัวบุคคลก่อนอนุญาตให้เข้าระบบ และกำหนดให้มีการทบทวนสิทธิเข้าถึงระบบสารสนเทศของผู้ใช้งานทุก ๑ ปี และมีการทบทวนสิทธิอย่างต่อเนื่อง โดย ศทก. ได้มีการเผยแพร่หลักเกณฑ์ระบบสารสนเทศ ทางเว็บไซต์ภายใน สปน. (Intranet) และหากมีการพัฒนาระบบสารสนเทศใหม่จะมีการแจ้งเวียนให้ผู้ใช้ระบบทราบต่อไป ๒.๔ การให้ความรู้ ความเข้าใจกับผู้ปฏิบัติงานอย่างต่อเนื่อง โดยดำเนินการดังนี้ (๑) เผยแพร่คู่มือระบบสารสนเทศ ทางเว็บไซต์ภายใน สปน. (Intranet) (๒) จัดฝึกอบรมให้ผู้ปฏิบัติงาน ในกรณีที่มีการพัฒนาระบบสารสนเทศ/ปรับปรุงใหม่หรือตามที่หน่วยงานภายใน สปน. ร้องขอ (๓) จัดประชุมชี้แจงการใช้งานระบบประชุมทางไกล ๒.๕ การเตรียมความพร้อมกรณีฉุกเฉิน พบว่า ศทก. มี Site สำรอง Co – Location ในกรณีที่ Site หลักไม่ทำงาน ได้มีการจัดทำแผนบริหารความเสี่ยงปีงบประมาณ พ.ศ. ๒๕๖๔ โดยกำหนดเป็นแผน	- ควรมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ระยะสั้น...

ผลการตรวจสอบ	ข้อเสนอแนะ
ระยะสั้น และ ศทก. ได้มีการทดสอบระบบให้อยู่ในสภาพพร้อมในการใช้งาน ประกอบด้วย (๑) ระบบสารสนเทศ ได้มีการทดสอบการใช้งานเป็นประจำทุก ๒ เดือน โดยมีการทดสอบครั้งสุดท้าย เมื่อวันที่ ๑๒ พ.ค. ๒๕๖๔ (๒) ระบบสำรองไฟฟ้า ได้มีการทดสอบระบบครั้งสุดท้าย เมื่อวันที่ ๒๐ มี.ค. ๒๕๖๔ (๓) แผนฉุกเฉิน ได้มีการซักซ้อมการปฏิบัติตามแผนบริหารความเสี่ยงกรณีเกิดเหตุเพลิงไหม้ ณ ห้องแม่ข่ายหรือลุกลามมาจากบริเวณอื่น เมื่อวันที่ ๑๓ ส.ค. ๒๕๖๓	
๓. การดำเนินการตามแผนงาน โครงการ และงบประมาณในการจัดหาและพัฒนาระบบงานสารสนเทศ ศทก. ได้รับจัดสรรงบประมาณเพื่อจัดหาและพัฒนาระบบสารสนเทศ ของ สปน. จำนวน ๒๕,๘๔๒,๖๒๐ บาท พบว่า ณ วันที่ ๓๑ พ.ค. ๒๕๖๔ มีผลการเบิกจ่ายทั้งสิ้น ๑๑,๒๖๙,๗๕๐ บาท คิดเป็นร้อยละ ๔๓.๖๑ สรุปได้ดังนี้ ๓.๑ การบำรุงรักษาระบบและอุปกรณ์ระบบสารสนเทศ จำนวน ๕ รายการ รวมเป็นเงิน ๑๔,๙๐๖,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๖,๒๑๙,๗๕๐ บาท ๓.๒ การจัดหาบริการคู่สายสัญญาณวงจรความเร็วสูงและบริการระบบประชุมทางไกลผ่านอินเทอร์เน็ต สปน. จำนวน ๒ รายการ รวมเป็นเงิน ๗,๐๐๐,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๓,๕๕๐,๐๐๐ บาท ๓.๓ การจัดหาครุภัณฑ์คอมพิวเตอร์ทดแทน ของ สปน. จำนวน ๘๓๖,๖๒๐ บาท ขณะนี้คณะกรรมการตรวจรับพัสดุอยู่ระหว่างการตรวจรับ ๓.๔ การจัดหาระบบบริหารจัดการเอกสารอิเล็กทรอนิกส์ ของ สปน. จำนวน ๒,๐๐๐,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๑,๕๐๐,๐๐๐ บาท ๓.๕ การปรับปรุงข้อมูลจราจรทางคอมพิวเตอร์ ขณะนี้อยู่ระหว่างการขออนุมัติโอนเปลี่ยนแปลงรายการงบประมาณเหลือจ่าย จำนวน ๑,๑๐๐,๐๐๐ บาท และอยู่ระหว่างการร่างขอบเขตงาน (TOR)	- ควรเร่งดำเนินการปรับปรุงข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้สามารถดำเนินการได้ทันภายในปีงบประมาณ พ.ศ. ๒๕๖๔

๓. ข้อเสนอ...

๓. **ข้อเสนอ**

จึงเรียนมาเพื่อโปรดทราบรายงานผลการตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๓ – พฤษภาคม ๒๕๖๔) เพื่อ กตน. จะได้แจ้งให้ ศทก. ทราบและดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางสายพิน สมบัติทอง)
นวก.ตน.ชพ. รกน.
ผอ.กตน.

- ทราบ และดำเนินการต่อไป
- ควรมีการตรวจสอบ และประเมินความเสี่ยงด้าน IT ที่อาจเกิดขึ้น อย่างน้อยปีละ ๑ ครั้ง และควรเร่งปรับปรุงข้อมูลการงาน

(นายธีรภัทร ประยูรสิทธิ)
ปลัดสำนักนายกรัฐมนตรี
๗ ก.ค. ๖๔

รหัสรายงานการตรวจสอบที่ ๑๕/๒๕๖๔

สำนักงานปลัดสำนักนายกรัฐมนตรี
กลุ่มตรวจสอบภายใน

รายงานผลการตรวจสอบ

หน่วยรับตรวจ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทก.) สำนักงานปลัดสำนักนายกรัฐมนตรี (สปน.)

เรื่องที่ตรวจสอบ การดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ 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. ๒๕๖๔ (เดือนตุลาคม ๒๕๖๓ – พฤษภาคม ๒๕๖๔)

ระยะเวลาการตรวจสอบ วันที่ ๖, ๒๐ – ๒๑ พฤษภาคม, ๔, ๑๐ – ๑๑, ๑๔ – ๑๕, ๒๑, ๒๔ - ๒๕, ๒๘ และ ๓๐ มิถุนายน ๒๕๖๔

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. ๒๕๖๔ (เดือนตุลาคม ๒๕๖๓ – พฤษภาคม ๒๕๖๔)

๔. สอบถามเจ้าหน้าที่ผู้รับผิดชอบและผู้ที่เกี่ยวข้อง

สรุปผลการตรวจสอบ

กตน. ได้ตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. ๒๕๖๔ ของ ศทก. สปน. (เดือนตุลาคม ๒๕๖๓ – พฤษภาคม ๒๕๖๔) สรุปได้ดังนี้

ผลการตรวจสอบ	ข้อเสนอแนะ
๑. นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ๑.๑ การจัดทำนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. เป็นลายลักษณ์อักษร ดังนี้ **(๑) นโยบาย** โดยมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๑) การเข้าถึงหรือการควบคุมการใช้สารสนเทศ ๒) การจัดระบบสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน และแผนเตรียมความพร้อมกรณีฉุกเฉิน และ ๓) จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ **(๒) ข้อปฏิบัติ** โดยมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๑) การควบคุมการเข้าถึงระบบสารสนเทศ/ระบบเครือข่าย/ระบบปฏิบัติการ ๒) การจัดการเข้าถึงและหน้าที่ความรับผิดชอบของผู้ใช้งาน ๓) การจัดทำระบบสำรองข้อมูลสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน และ ๔) การตรวจสอบและประเมินความเสี่ยง ๑.๒ สปน. ได้มีประกาศสำนักนายกรัฐมนตรี เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และนโยบายคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์ ของ สปน. ลงวันที่ ๒๐ เม.ย. ๒๕๕๕ อย่างไรก็ดี พบว่า ไม่มีประกาศฯ ให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ ๑.๓ การกำหนดผู้รับผิดชอบเป็นกลุ่มงาน แต่ยังไม่ได้มีการระบุผู้รับผิดชอบในแต่ละด้านเป็นรายบุคคล เช่น (๑) กลุ่มงานบริหารเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบด้านระบบเครือข่ายและการซ่อมบำรุง และ (๒) กลุ่มงานบริหารระบบฐานข้อมูลสารสนเทศ เป็นผู้รับผิดชอบด้านระบบสารสนเทศของ สปน. เป็นต้น	- ควรมีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ให้เป็นปัจจุบันอยู่เสมอ - ควรมีการประกาศนโยบายและข้อปฏิบัติให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ - ควรมีการกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติให้ชัดเจน เช่น มีคำสั่งหรือหนังสือมอบหมายสั่งการโดยระบุบุคคลผู้รับผิดชอบให้ชัดเจน

ผลการตรวจสอบ	ข้อเสนอแนะ
๒. การดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ๒.๑ การควบคุมความปลอดภัยทางกายภาพ ของ ศูนย์สารสนเทศ ห้องเก็บสารสนเทศและห้องทำงาน ของ ศทก. พบว่า (๑) มีการปิดล็อกเมื่อไม่มีการใช้งาน และจัดเก็บอุปกรณ์ ครุภัณฑ์ ในตู้ที่มีการควบคุมกุญแจพร้อมทั้งมีทะเบียนคุมการเบิกจ่าย (๒) มีการควบคุมการเข้า – ออกในพื้นที่เฉพาะโดยมอบหมายเจ้าหน้าที่กลุ่มงานตามภารกิจงานในแต่ละด้านที่รับผิดชอบ ซึ่งยังไม่มีคำสั่งหรือการมอบหมายสั่งการเพื่อระบุตัวบุคคลแต่อย่างใด (๓) มีการควบคุมเพื่อป้องกันการบุกรุกโจมตีโดยติดตั้ง Firewall และมีการซักซ้อมแผนฉุกเฉินกรณีไฟไหม้ ปีละ ๑ ครั้ง (๔) มีการทำสัญญาจ้างกับบริษัท ไซท์เพรพพาเรชั่น แมเนจเมนท์ จำกัด เพื่อบำรุงรักษาอุปกรณ์ไฟฟ้าในห้อง Data Center และตรวจสอบการทำงานทุก ๓ เดือน และทำสัญญาจ้าง บริษัท ซีเอสล็อกซอินโฟ จำกัด (มหาชน) เพื่อให้บริการคู่สายสัญญาณวงจรความเร็วสูงเพื่อใช้บริการอินเทอร์เน็ตและบำรุงรักษาซ่อมแซมเครื่องมือ วัสดุและอุปกรณ์ที่ให้บริการทุกชนิด ทั้งนี้ ศทก. ยังไม่มีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบ ๒.๒ การควบคุมด้านข้อมูลและสารสนเทศ ศทก. พบว่า มีการกำหนดสิทธิการเข้าถึงให้กับอุปกรณ์คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ ในการใช้บริการระบบเครือข่ายไร้สาย (OPM WiFi) ของ สปน. และมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้จำนวนไม่น้อยกว่า ๙๐ วัน	- ควรมีคำสั่งหรือหนังสือมอบหมายสั่งการโดยระบุบุคคลผู้รับผิดชอบการเข้า – ออกในพื้นที่เฉพาะให้ชัดเจน - ควรมีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงานเพื่อให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ให้กับผู้ใช้งานทราบทั่วกัน

ผลการตรวจสอบ	ข้อเสนอแนะ
ทั้งนี้ ศทก. อยู่ระหว่างดำเนินการจัดซื้ออุปกรณ์จัดเก็บ Log File มาทดแทน เนื่องจากอุปกรณ์ที่ใช้อยู่ปัจจุบันมีอายุการใช้งานมากกว่า ๑๐ ปี และได้ดำเนินการเกี่ยวกับข้อมูลและสารสนเทศโดยกำหนดไว้ในนโยบายและข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สปน. ดังนี้ (๑) การจัดประเภทของข้อมูล เช่น ข้อมูลภายนอกสามารถเปิดเผยได้ ในส่วนข้อมูลภายในเป็นไปตามลำดับชั้นความลับของข้อมูล (๒) การจัดชั้นความลับของข้อมูล ศทก. ไม่มีการกำหนดชั้นความลับของข้อมูลไว้ ในส่วนของข้อมูลลับจะไม่มีการนำข้อมูลเข้าสู่ระบบสารสนเทศ (๓) การจัดชั้นการเข้าถึงเป็นไปตามลำดับชั้นความลับของข้อมูล เช่น ระบบงานบริหารงานบุคคล (๔) การกำหนดเวลาในการเข้าถึง ศทก. ได้กำหนดเวลาการเข้าถึงข้อมูลบางระบบที่มีความจำเป็น เช่น การเข้าใช้ประโยชน์ข้อมูลทะเบียนประวัติราษฎร (๕) การกำหนดช่องทางในการเข้าถึง ศทก. ได้กำหนดช่องทางให้ผู้ใช้เข้าถึงระบบได้ตามความเหมาะสม โดยแบ่งเป็น ๒ ช่องทาง ได้แก่ ๑) ระบบสำหรับเจ้าหน้าที่ สปน. ๒) ระบบสำหรับบุคคลทั่วไป ๒.๓ การควบคุมและจำกัดสิทธิผู้ใช้ระบบ พบว่ามีการกำหนดสิทธิในการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่โดยหน่วยงานต้นสังกัดต้องทำหนังสือถึง ศทก. เป็นลายลักษณ์อักษร และมอบหมายให้ผู้ใช้ระบบเข้าถึงระบบเฉพาะของหน่วยงาน ตลอดจนการเพิ่มเติม/ยกเลิกสิทธิการเข้าใช้ระบบงานของเจ้าหน้าที่ที่ได้รับมอบหมาย โดย ศทก. จะมีหนังสือแจ้งหน่วยงานต้นสังกัด พร้อมแนบรหัสผ่านรายบุคคลด้วยการจัดใส่ซองปิดผนึกและเซ็นชื่อกำกับบริเวณผนึก และมีการกำหนดการเพิกถอนสิทธิ และเงื่อนไขให้ผู้ใช้ระบบต้องเก็บรักษารหัสผ่านของตนเองและของกลุ่มงานไว้เป็นความลับ และเนื่องจากระบบสารสนเทศบางระบบมีความจำเป็นต้องใช้ User ร่วม เพื่อเข้าถึงข้อมูลของ	

ผลการตรวจสอบ	ข้อเสนอแนะ
แต่ละกลุ่มงานหรือหน่วยงานด้วย User เดียวกัน จะไม่มีการจัดเก็บข้อมูลเฉพาะบุคคล และผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการที่ได้รับสิทธิเท่านั้น ในกรณีที่ผู้ใช้งานจากภายนอกเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน จะมีกระบวนการในการยืนยันตัวบุคคลก่อนอนุญาตให้เข้าระบบ และกำหนดให้มีการทบทวนสิทธิเข้าถึงระบบสารสนเทศของผู้ใช้งานทุก ๑ ปี และมีการทบทวนสิทธิอย่างต่อเนื่อง โดย ศทก. ได้มีการเผยแพร่หลักเกณฑ์ระบบสารสนเทศ ทางเว็บไซต์ภายใน สปน. (Intranet) และหากมีการพัฒนาระบบสารสนเทศใหม่จะมีการแจ้งเวียนให้ผู้ใช้ระบบทราบต่อไป ๒.๔ การให้ความรู้ ความเข้าใจกับผู้ปฏิบัติงานอย่างต่อเนื่อง โดยดำเนินการดังนี้ (๑) เผยแพร่คู่มือระบบสารสนเทศ ทางเว็บไซต์ภายใน สปน. (Intranet) (๒) จัดฝึกอบรมให้ผู้ปฏิบัติงาน ในกรณีที่มีการพัฒนาระบบสารสนเทศ/ปรับปรุงใหม่หรือตามที่หน่วยงานภายใน สปน. ร้องขอ (๓) จัดประชุมชี้แจงการใช้งานระบบประชุมทางไกล	
๒.๕ การเตรียมความพร้อมกรณีฉุกเฉิน พบว่า ศทก. มี Site สำรอง Co – Location ในกรณีที่ Site หลักไม่ทำงาน ได้มีการจัดทำแผนบริหารความเสี่ยงปีงบประมาณ พ.ศ. ๒๕๖๔ โดยกำหนดเป็นแผนระยะสั้น และ ศทก. ได้มีการทดสอบระบบให้อยู่ในสภาพพร้อมในการใช้งาน ประกอบด้วย (๑) ระบบสารสนเทศ ได้มีการทดสอบการใช้งานเป็นประจำทุก ๒ เดือน โดยมีการทดสอบครั้งสุดท้าย เมื่อวันที่ ๑๒ พ.ค. ๒๕๖๔ (๒) ระบบสำรองไฟฟ้า ได้มีการทดสอบระบบครั้งสุดท้าย เมื่อวันที่ ๒๐ มี.ค. ๒๕๖๔ (๓) แผนฉุกเฉิน ได้มีการซักซ้อมการปฏิบัติตามแผนบริหารความเสี่ยงกรณีเกิดเหตุเพลิงไหม้ ณ ห้องแม่ข่ายหรือลุกลามมาจากบริเวณอื่น เมื่อวันที่ ๑๓ ส.ค. ๒๕๖๓	- ควรมีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ผลการตรวจสอบ	ข้อเสนอแนะ
๓. การดำเนินการตามแผนงาน โครงการ และงบประมาณในการจัดหาและพัฒนาระบบงานสารสนเทศ ศทก. ได้รับจัดสรรงบประมาณเพื่อจัดหาและพัฒนาระบบสารสนเทศ ของ สปน. จำนวน ๒๕,๘๔๒,๖๒๐ บาท พบว่า ณ วันที่ ๓๑ พ.ค. ๒๕๖๔ มีผลการเบิกจ่ายทั้งสิ้น ๑๑,๒๖๙,๗๕๐ บาท คิดเป็นร้อยละ ๔๓.๖๑ สรุปได้ดังนี้ ๓.๑ การบำรุงรักษาระบบและอุปกรณ์ระบบสารสนเทศ จำนวน ๕ รายการ รวมเป็นเงิน ๑๔,๙๐๖,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๖,๒๑๙,๗๕๐ บาท ๓.๒ การจัดหาบริการคู่สายสัญญาณวงจรความเร็วสูงและบริการระบบประชุมทางไกลผ่านอินเทอร์เน็ต สปน. จำนวน ๒ รายการ รวมเป็นเงิน ๗,๐๐๐,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๓,๕๕๐,๐๐๐ บาท ๓.๓ การจัดหาครุภัณฑ์คอมพิวเตอร์ทดแทนของ สปน. จำนวน ๘๓๖,๖๒๐ บาท ขณะนี้คณะกรรมการตรวจรับพัสดุอยู่ระหว่างการตรวจรับ ๓.๔ การจัดหาระบบบริหารจัดการเอกสารอิเล็กทรอนิกส์ ของ สปน. จำนวน ๒,๐๐๐,๐๐๐ บาท ซึ่งมีผลการเบิกจ่าย ๑,๕๐๐,๐๐๐ บาท ๓.๕ การปรับปรุงข้อมูลจราจรทางคอมพิวเตอร์ ขณะนี้อยู่ระหว่างการขออนุมัติโอนเปลี่ยนแปลงรายการงบประมาณเหลือจ่าย จำนวน ๑,๑๐๐,๐๐๐ บาท และอยู่ระหว่างการร่างขอบเขตงาน (TOR)	- ควรเร่งดำเนินการปรับปรุงข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้สามารถดำเนินการได้ทันภายในปีงบประมาณ พ.ศ. ๒๕๖๔

ผู้ตรวจสอบ
(นางสกาวรัตน์ ทองเทพ)
นวก.ตน.ชพ.
๗ ก.ค. ๒๕๖๔

ผู้กำกับดูแลการตรวจสอบ
(นางสายพิน สมบัติทอง)
นวก.ตน.ชพ. รกน.
ผอ.กตน.
๗ ก.ค. ๒๕๖๔