ที่ นร ๑๒๐๐/ว๑๘

สำนักงาน ก.พ.ร.
ถนนพิษณุโลก กทม. ๑๐๓๐๐

๑๗ มีนาคม ๒๕๖๙

เรื่อง การประเมินความคุ้มค่าเพื่อพัฒนาองค์การมหาชนตามมติคณะรัฐมนตรี

เรียน เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

อ้างถึง หนังสือสำนักงาน ก.พ.ร. ที่ นร ๑๒๐๐/ว๑๔ ลงวันที่ ๒๓ กุมภาพันธ์ ๒๕๖๙

สิ่งที่ส่งมาด้วย มติคณะทำงานกลั่นกรองการประเมินความคุ้มค่าเพื่อพัฒนาองค์การมหาชน

ตามหนังสือที่อ้างถึง สำนักงาน ก.พ.ร. ได้เชิญท่านเข้าร่วมนำเสนอและให้ข้อมูลรายละเอียดของห่วงโซ่ผลการดำเนินงาน (result chain) และความสัมพันธ์ขององค์การมหาชนในระบบนิเวศ (ecosystem) ต่อคณะทำงานกลั่นกรองการประเมินความคุ้มค่าเพื่อพัฒนาองค์การมหาชน เมื่อวันที่ ๔ มีนาคม ๒๕๖๙ ณ ห้องประชุม ๕๐๓ สำนักงาน ก.พ.ร. นั้น

คณะทำงานฯ ในการประชุมครั้งที่ ๑/๒๕๖๙ เมื่อวันที่ ๔ มีนาคม ๒๕๖๙ ได้พิจารณา result chain และ ecosystem ขององค์การมหาชนแล้ว มีมติเห็นชอบให้องค์การมหาชนนำความเห็นของคณะทำงานฯ ไปปรับปรุงรายละเอียดบันทึกข้อตกลงการประเมินความคุ้มค่าเพื่อพัฒนาองค์การมหาชน และให้รับความเห็นของคณะทำงานในส่วนข้อเสนอเพื่อการพัฒนาไปพิจารณาดำเนินการต่อไป รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ทั้งนี้ ให้องค์การมหาชนเสนอคณะกรรมการองค์การมหาชนพิจารณาและจัดส่งไปยังสำนักงาน ก.พ.ร. ภายในวันที่ ๑๕ พฤษภาคม ๒๕๖๙ เพื่อเสนอ อ.กพม. ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นางสาวจิตตา กิตติเสถียรนนท์)
รองเลขาธิการ ก.พ.ร. ปฏิบัติราชการแทน
เลขาธิการ ก.พ.ร.

กองกิจการองค์การมหาชนและหน่วยงานของรัฐรูปแบบอื่น
โทร. ๐ ๒๓๕๖ ๙๙๙๙ ต่อ ๘๙๐๓ (ปนัดดา) และ ๘๙๖๙ (นิธินุช)
ไปรษณีย์อิเล็กทรอนิกส์ saraban@opdc.go.th

คณะทำงานกลั่นกรองการประเมินความคุ้มค่าเพื่อพัฒนาองค์การมหาชน
วันพุธที่ ๔ มีนาคม ๒๕๖๙
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ความเห็นต่อ ecosystem

- **ควรขยายความ "กลไกการสร้างความเชื่อมั่นไว้วางใจระหว่างประเทศ (CBM)"** ให้เห็นภาพชัดเจนว่ามีบทบาทสำคัญต่อการยกระดับความปลอดภัยไซเบอร์ของประเทศและมีผลโดยตรงต่อตัวชี้วัดผลกระทบ (Global Cybersecurity Index ของประเทศ) ตามที่ตั้งเป้าหมายไว้
- **ควรเพิ่มเติมความเชื่อมโยงระหว่างกระบวนการของ สกมช. กับบทบาทของ สพธอ.** ในส่วนที่ สพธอ. รับข้อมูลจาก สกมช. หรือหน่วยงานที่เกี่ยวข้องเพื่อนำไปใช้ในการกำหนด/ปรับปรุงหลักเกณฑ์/มาตรฐานความปลอดภัยของระบบธุรกรรมออนไลน์
- ควรระบุชื่อหน่วยงานต่างประเทศที่มีความร่วมมือให้ชัดเจนในแต่ละกิจกรรม เช่น การแบ่งปันข้อมูล การพัฒนาบุคลากร เพื่อให้เห็นบทบาทของความร่วมมือชัดเจนขึ้น

ความเห็นต่อ result chain

- **ภาพรวม**
  - **ควรทบทวนตัวชี้วัดให้สะท้อนเป้าหมายการมีอยู่ของ สกมช.** ในระบบนิเวศด้านความมั่นคงปลอดภัยไซเบอร์ **ที่แสดงถึงผลลัพธ์เชิงนโยบายและความสำเร็จที่ประเทศจะได้รับอย่างเป็นรูปธรรม** อาทิ ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศที่เพิ่มขึ้น การลดความเสี่ยงและผลกระทบจากภัยคุกคามทางไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงการยกระดับการยอมรับมาตรฐานและบทบาทของประเทศไทยในเวทีความมั่นคงปลอดภัยไซเบอร์ระดับสากล
  - **ควรกำหนดตัวชี้วัดให้สอดคล้องกับงบประมาณ**ที่ได้รับการจัดสรรโดยสะท้อนความคุ้มค่าและ**ประสิทธิภาพในการใช้ทรัพยากรเพื่อบรรลุภารกิจหลักของ สกมช.** เช่น ความสามารถในการป้องกัน การรับมือ และการฟื้นฟูจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนผลลัพธ์ที่เกิดขึ้นต่อหน่วยงานภาครัฐ ภาคเอกชน และประชาชนโดยรวม เพื่อให้เห็นความสอดคล้องเชื่อมโยงจากงบประมาณที่ได้รับไปสู่การกำหนดกระบวนการ (Process) ไปสู่ผลผลิต (Output) แล้วต่อยอดให้เกิดผลลัพธ์ (Outcome) และผลกระทบ (Impact) ที่วัดการเปลี่ยนแปลงจริง เช่น ระดับความพร้อมและความสามารถในการรับมือเหตุไซเบอร์ของหน่วยงาน ไม่วัดเพียงจำนวนกิจกรรมหรือผู้เข้าร่วม
  - ควรระบุข้อมูลพื้นฐาน (baseline) และทบทวนค่าเป้าหมาย ให้สอดคล้องกับผลการดำเนินงานที่ผ่านมา (ทุกตัวชี้วัด)
- **ตัวชี้วัดผลลัพธ์ (Outcome)**
  - **ควรเพิ่มเติมตัวชี้วัดที่สะท้อนผลจากการดำเนินงานเชิงปฏิบัติการโดยตรง** เช่น การรับมือเหตุการณ์ไซเบอร์ การแลกเปลี่ยนข้อมูลภัยคุกคาม การทำงานของ CII และ ThaiCERT ตลอดจนกลไกสนับสนุนด้านเทคนิค เพื่อให้เห็นผลลัพธ์ที่วัดได้ในระยะยาว ทั้งมิติการป้องกันและมิติการตอบสนองภัยคุกคามของประเทศ ซึ่งอาจวัดผลได้จาก ๔ ประเด็น ได้แก่ ๑) การลดผลกระทบที่เกิดจากการถูกโจมตี ๒) ระยะเวลามาตรฐานในการกู้คืนระบบ ๓) การค้นหาสาเหตุ

ของการถูกโจมตี ๔) การสร้างความร่วมมือและการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมกลุ่มเป้าหมายหรือสร้างผลกระทบที่สำคัญของประเทศ

- **ควรเพิ่มเติมตัวชี้วัดที่ส่งผลต่อความเชื่อมั่น/ความเชื่อใจ (trust) ของประชาชน**ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ เช่น ระยะเวลามาตรฐานที่สามารถกู้คืนระบบได้จากการถูกโจมตี
- **ควรปรับตัวชี้วัดที่มีลักษณะเป็นตัวชี้วัดระดับผลผลิตให้เป็นตัวชี้วัดที่สะท้อนผลลัพธ์ของการดำเนินการ** เช่น "ร้อยละของจำนวนหน่วยงานเป้าหมาย มีการดำเนินงานที่สอดคล้องต่อนโยบายและแผนปฏิบัติการฯ" "ร้อยละของหน่วยงานได้รับการสนับสนุนในการรับมือจากภัยคุกคามทางไซเบอร์เทียบกับที่ร้องขอ" "ยอดสะสมของจำนวนผู้ที่ผ่านแบบทดสอบ E-learning และ Platform online ของ สกมช."
- **ควรรวมตัวชี้วัดที่วัดการดำเนินการตามกำหนดเวลาเป็นตัวชี้วัดเดียวกัน** เช่น ร้อยละความสำเร็จของการแจ้งเตือนจากการเฝ้าระวังและแจ้งเตือนภายใน ๒ วันทำการ
- **ควรปรับค่าเป้าหมายให้ท้าทายมากขึ้นในตัวชี้วัดที่สำคัญ** เช่น "ร้อยละของ CII ที่มีการดำเนินงานตามมาตรา ๕๔ ผ่านเกณฑ์ประเมินของ สกมช." "ระดับความสำเร็จของหน่วยงานเป้าหมายมี Platform สำหรับรับและแบ่งปันข้อมูลทางไซเบอร์"

- **ตัวชี้วัดผลกระทบ (Impact)**
  - **ควรทบทวนค่าเป้าหมายตัวชี้วัด Global Cybersecurity Index** (เป้าหมาย ๙๕ คะแนน) เนื่องจากคะแนนปี ๒๕๖๗ สูงถึง ๙๙.๒๒ คะแนน จึงควรปรับวิธีตั้งค่าเป้าหมายให้ท้าทายและสะท้อนผลการดำเนินงานมากขึ้น เช่น มิติของอันดับหรือการจัด tier แทนการดูเฉพาะคะแนน รวมทั้งเพิ่มเติมคำอธิบายว่าตัวชี้วัดเชื่อมโยงกับเป้าหมายการมีอยู่อย่างไร

ข้อเสนอเพื่อการพัฒนา

- **ควรมุ่งเน้นการยกระดับความสามารถของหน่วยงานในการฟื้นฟูระบบให้กลับมาใช้งานได้ตามปกติหลังเกิดเหตุโจมตี** (Recovery) รวมถึงความพร้อมด้านการสำรองและกู้คืนข้อมูล (Backup & Restore) อย่างมีประสิทธิภาพ ตัวชี้วัดที่สะท้อน Impact จริง เช่น ระยะเวลาในการกู้คืนระบบ (Recovery Time) การลดความเสียหายจากเหตุไซเบอร์ และความต่อเนื่องในการให้บริการประชาชน ซึ่งแสดงถึงความทนทานและความเชื่อมั่นต่อระบบดิจิทัลของประเทศในระยะยาว
- **ควรพัฒนาระบบการจัดเก็บและรายงานข้อมูลที่เกี่ยวข้องให้เป็นระบบและตรวจสอบได้มากขึ้น** โดยจัดเก็บสถิติข้อมูลการถูกโจมตีในแต่ละครั้งและประเมินค่าความเสียหาย และจัดทำฐานข้อมูลแหล่งที่มาของการโจมตีเพื่อสร้างแนวทางการป้องกัน ซึ่งบางส่วนอาจเป็นข้อมูลลับ เพื่อให้สามารถสรุปผลตัวชี้วัดผลกระทบที่สำคัญในภาพรวมได้อย่างเป็นรูปธรรม เช่น มูลค่าความเสียหายต่อเหตุการณ์ มูลค่าความเสียหายรวมในแต่ละปี หรือค่าใช้จ่ายในการกู้คืนระบบต่อเคส ซึ่งจะช่วยสะท้อนผลกระทบที่แท้จริงของภัยไซเบอร์ได้ชัดเจนยิ่งขึ้น
- **ควรพิจารณาให้มีการเปิดเผยข้อมูลในระดับสถิติภาพรวม** (โดยไม่ระบุชื่อผู้เสียหายหรือหน่วยงาน) เพื่อเพิ่มความโปร่งใส และสนับสนุนการประเมินเชิงนโยบาย ทั้งยังช่วยสร้างความเชื่อมั่นต่อการดำเนินงานของ สกมช. ได้มากกว่าการรายงานเฉพาะขั้นตอนการกู้ระบบโดยไม่มีข้อมูลผลกระทบเชิงมูลค่า

- **สกมช. ควรเป็นหน่วยงานต้นแบบหรือสร้างหน่วยงานต้นแบบ** ในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ โดย**ถอดบทเรียน (Practice) ที่สำคัญจาก Global Cybersecurity Index** มาประยุกต์ใช้ในการพัฒนาเครื่องมือมาตรฐานเพื่อยกระดับขีดความสามารถของประเทศในการป้องกัน รับมือ และฟื้นฟูจากภัยคุกคามได้อย่างมีประสิทธิภาพและเป็นรูปธรรม สำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเผยแพร่ให้กับหน่วยงานที่เกี่ยวข้องนำไปใช้