รายงานความคืบหน้าการดำเนินงานสมาร์ทกริด
แผนอำนวยการสนับสนุนการขับเคลื่อน (การบริหารการขับเคลื่อน)
หน่วยงาน : สำนักงานนโยบายและแผนพลังงาน

หัวข้อ	รายละเอียด
1. ชื่อโครงการ	การพัฒนาระบบรักษาความมั่นคงความปลอดภัยด้านไซเบอร์ (Cybersecurity) (EPPO-02)
2. ความเป็นมา/หลักการเหตุผล	สำนักงานนโยบายและแผนพลังงาน (สนพ.) ได้จัดทำแผนขับเคลื่อนการดำเนินงานด้านสมาร์ทกริดของประเทศไทย ในระยะสั้น พ.ศ. 2560–2564 ซึ่งมีความสอดคล้องกับกรอบการดำเนินงานในระยะสั้น ตามแผนแม่บทการพัฒนาระบบโครงข่ายสมาร์ทกริดของประเทศไทย พ.ศ. 2558–2579 และนำเสนอต่อคณะอนุกรรมการเพื่อศึกษาแนวทางการพัฒนาระบบโครงข่ายไฟฟ้าอัจฉริยะ (Smart Grid) และคณะกรรมการบริหารนโยบายพลังงาน (กบง.) ทั้งนี้ กพช. เมื่อวันที่ 8 ธันวาคม 2559 ได้เห็นชอบแผนขับเคลื่อนการดำเนินงานด้านสมาร์ทกริดของประเทศไทยในระยะสั้น พ.ศ. 2560–2564 รวมทั้งเห็นชอบกรอบงบประมาณการดำเนินการตามแผนฯ โดยกำหนดกรอบการพัฒนาและขับเคลื่อน 5 เทคโนโลยีหลัก โดยแบ่งออกเป็น 3 เสาหลัก ประกอบด้วย • **เสาหลักที่ 1** : การตอบสนองด้านความต้องการไฟฟ้าและระบบบริหารจัดการพลังงาน (DR & EMS) • **เสาหลักที่ 2** : ระบบพยากรณ์ไฟฟ้าที่ผลิตได้จากพลังงานหมุนเวียน (RE Forecast) • **เสาหลักที่ 3** : ระบบโครงข่ายไฟฟ้าขนาดเล็กและระบบกักเก็บพลังงาน (Micro Grid & ESS) ทั้งนี้ ภายใต้แผนการขับเคลื่อนการดำเนินงานด้านสมาร์ทกริดของประเทศไทยในระยะสั้น (พ.ศ. 2560–2564) ได้ระบุภารกิจที่ สนพ. จะต้องดำเนินการพัฒนาระบบรักษาความมั่นคงความปลอดภัยด้านไซเบอร์ (Cyber Security) ซึ่งความปลอดภัยของระบบโครงข่ายสมาร์ทกริดภายในระบบไฟฟ้าเป็นสิ่งสำคัญที่หลีกเลี่ยงไม่ได้ เพื่อที่จะรักษาการทำงานของระบบผลิตและส่งจ่ายไฟฟ้าให้มีเสถียรภาพและเชื่อถือได้อย่างต่อเนื่อง เมื่อระบบโครงข่ายสมาร์ทกริดมีความปลอดภัยสูงขึ้น ก็จะส่งผลให้โอกาสที่จะเกิดปัญหาไฟฟ้าดับลดน้อยลงตามไปด้วย และหากไม่มีการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมอาจนำไปสู่ปัญหาไฟฟ้าดับในวงกว้างตามมา ดังนั้น เพื่อเป็นการปกป้องโครงสร้างพื้นฐานของระบบโครงข่ายสมาร์ทกริดที่มีความสำคัญนี้ และเพื่อให้แน่ใจว่าสามารถส่งจ่ายไฟฟ้าได้อย่างน่าเชื่อถือและต่อเนื่องให้กับผู้ใช้ปลายทาง ความปลอดภัยของระบบโครงข่ายสมาร์ทกริดนั้นจะต้องถูกพิจารณาและให้ความสำคัญในลำดับต้นๆ ในอนาคตโครงสร้างพื้นฐานทางไฟฟ้าจะต้องได้รับการปรับปรุงให้ทันสมัยด้วยระบบสมาร์ทกริดเพื่อรองรับพลังงานหมุนเวียน และผลจาก Disruptive Technology เช่น Mircogrid Prosumer โดยเป็นระบบที่รวมเอาทั้งฟังก์ชั่นการทำงานพื้นฐานในปัจจุบันและฟังก์ชั่นที่มีความซับซ้อนเพิ่มขึ้นในอนาคตเข้าไว้ด้วยกัน ซึ่งต้องอาศัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology: ICT) เข้ามาผสมผสานอย่างหลีกเลี่ยงมิได้ ความปลอดภัยของระบบสมาร์ทกริดจึงมิใช่แค่การพิจารณาความปลอดภัยในมิติเชิงกายภาพเท่านั้น แต่ต้องพิจารณาถึงความมั่นคงความปลอดภัยด้านไซเบอร์ควบคู่ไปด้วย แม้ว่าการนำระบบไซเบอร์เข้ามาใช้งานจะทำให้สามารถบริหารจัดการโครงข่ายไฟฟ้าที่มีความซับซ้อนได้ชาญฉลาดและมีประสิทธิภาพยิ่งขึ้น แต่ก็จะมีปัญหาประเด็นการโจมตีทางไซเบอร์เพิ่มเข้ามาเช่นเดียวกัน อันอาจก่อให้เกิดความล้มเหลวในการดำเนินงานและท้ายที่สุดนำมาสู่ปัญหาไฟฟ้าดับตามมา

หัวข้อ	รายละเอียด
3. วัตถุประสงค์	3.1 เพื่อประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของไทย 3.2 เพื่อเสนอแนะการปรับเปลี่ยน นโยบาย กฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้องที่เหมาะสมในการป้องกันภัยคุกคามทางไซเบอร์สำหรับงานด้านสมาร์ทกริดของประเทศไทย 3.3 เพื่อจัดทำแผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริด
4. ขอบเขต/วิธีการดำเนินโครงการ	4.1 ศึกษาทบทวนข้อมูลภัยคุกคามทางไซเบอร์ด้านระบบไฟฟ้า มาตรการปกป้องและหรือป้องกันระบบไฟฟ้าในต่างประเทศ ซึ่งครอบคลุมประเด็นต่างๆ ได้แก่ - ความสำคัญและความจำเป็นในการปกป้องและหรือป้องกันด้านระบบไฟฟ้าจากภัยคุกคามไซเบอร์ - ประเภทของภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นต่อด้านระบบไฟฟ้า - แนวทางการศึกษาและตัวอย่างการประเมินความเสี่ยงต่อระบบไฟฟ้าจากภัยคุกคามทางไซเบอร์ - กรณีศึกษา รูปแบบภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าที่เกิดขึ้นในต่างประเทศ 4.2 ศึกษาแนวทาง นโยบาย กฎหมาย มาตรฐาน ระเบียบ การกำหนดมาตรการ แผนการดำเนินงานและเทคโนโลยีที่เกี่ยวข้องในการดำเนินการป้องกันภัยคุกคามทางไซเบอร์สำหรับระบบไฟฟ้าต่างประเทศ 4.3 ศึกษาวิเคราะห์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกี่ยวข้องกับระบบไฟฟ้าในปัจจุบัน และแนวโน้มการปรับเปลี่ยนระบบเทคโนโลยีสารสนเทศและการสื่อสารในอนาคตภายใต้การดำเนินงานด้านสมาร์ทกริดของไทย 4.4 ศึกษาและประเมินระดับความเสี่ยงของภัยคุกคามทางไซเบอร์ต่อระบบไฟฟ้าของไทยในปัจจุบันรวมทั้งอนาคตภายใต้การดำเนินงานด้านสมาร์ทกริดของไทย จากการวิเคราะห์และประเมินในเรื่องต่างๆ ดังนี้ - วิเคราะห์ประเภทของภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นต่อการควบคุมระบบไฟฟ้าของไทย (โครงข่ายไฟฟ้าและโครงสร้างพื้นฐาน) ผ่านกระบวนการวิเคราะห์แรงจูงใจและมูลเหตุอื่นที่เกี่ยวข้อง - วิเคราะห์ผลกระทบของภัยคุกคามทางไซเบอร์ที่มีต่อระบบไฟฟ้าของไทย - วิเคราะห์/ประเมินความเป็นไปได้ของผู้คุกคามทางไซเบอร์และแนวทางในการคุกคามทางไซเบอร์ต่อระบบไฟฟ้า - วิเคราะห์ Attack Surface ของระบบไฟฟ้าของไทย ซึ่งสามารถถูกคุกคามได้ทางไซเบอร์ - วิเคราะห์การเข้าถึงข้อมูลของระบบไฟฟ้าของไทยต่อโลกไซเบอร์ ทั้งนี้ให้ครอบคลุมช่องทางอื่นๆ ที่ไม่ใช่ระบบเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ตด้วย - วิเคราะห์รูปแบบและแนวทางปกป้องและหรือป้องกันภัยคุกคามทางไซเบอร์ที่มีอยู่ในปัจจุบันรวมถึงที่จะมีขึ้นสำหรับงานด้านสมาร์ทกริดของประเทศไทย ว่ามีประสิทธิผลมากน้อยเพียงใด โดยรวมถึงการวิเคราะห์ความคุ้มค่าในการดำเนินมาตรการการปกป้องและหรือป้องกันภัยคุกคามทางไซเบอร์ (Cost tradeoff) 4.5 กำหนดกรอบขอบเขตและแนวทางของการรักษาความปลอดภัยด้านไซเบอร์สำหรับระบบไฟฟ้าของไทยรวมถึงการดำเนินงานด้านสมาร์ทกริดของไทยที่จะเกิดขึ้นในอนาคตใน 3 มิติ ได้แก่ - การรักษาความลับ (Confidentiality) เช่น ข้อมูลการใช้งานพลังงานไฟฟ้ารายบุคคล ข้อมูลโครงข่าย เป็นต้น - การรักษาความครบถ้วน (Integrity) เช่น ระดับความเชื่อถือได้ของระบบไฟฟ้า ความถูกต้องของการวัดการจ่ายไฟฟ้า ความถูกต้องของบิลค่าไฟฟ้า เป็นต้น

หัวข้อ	รายละเอียด
	- การรักษาสภาพพร้อมใช้งาน (Availability) เช่น ระบบสำคัญที่ควบคุมการจ่ายไฟฟ้า ระบบที่เก็บข้อมูลที่จำเป็นในการใช้ควบคุมโครงข่ายไฟฟ้า เป็นต้น 4.6 ศึกษาวิเคราะห์นโยบาย กฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้อง และเสนอแนะการปรับเปลี่ยนให้เหมาะสมในการปกป้องและหรือป้องกันภัยคุกคามทางไซเบอร์สำหรับงานด้านสมาร์ทกริดของประเทศไทย 4.7 เสนอแนะโครงสร้างการบริหารจัดการทั้งในระยะสั้นและระยะยาว รวมถึงบทบาทหน้าที่เพื่อดำเนินการและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับระบบสมาร์ทกริดอย่างต่อเนื่อง 4.8 จัดทำแผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสมาร์ทกริดให้สอดคล้องกับแผนแม่บทสมาร์ทกริดของประเทศไทยและกฎระเบียบที่เกี่ยวข้อง ซึ่งประกอบไปด้วยอย่างน้อย ด้านเทคโนโลยี ด้านการพัฒนาบุคลากร รวมถึงผลิตเอกสารเพื่อเผยแพร่
5. แผนและระยะเวลาดำเนินโครงการ	ระยะเวลาดำเนินโครงการ 18 เดือน ระหว่างปี พ.ศ. 2562-2564 (ก.ค.62–ม.ค.64) (ซึ่งมีการขยายระยะเวลาดำเนินการเพิ่มเติมจากแผนการขับเคลื่อนฯ ที่ระบุไว้ปี พ.ศ. 2560-2561)
6. สถานที่ตั้ง/สถานที่ดำเนินโครงการ	สำนักงานนโยบายและแผนพลังงาน
7. งบประมาณ	งบประมาณรวม 15.8 ล้านบาท
8. สรุปความคืบหน้าในการดำเนินงาน (ณ มกราคม 64)	สนพ. ได้ดำเนินการศึกษาแล้วเสร็จ โดยได้จัดทำ (ร่าง) แผนการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับภาคส่วนไฟฟ้า โดยแบ่งออกเป็น 4 ส่วน ดังนี้ 1) การบริหารจัดการเชิงนโยบายและโครงสร้างการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า - กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ - กำหนดมาตรฐานขั้นต่ำและประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - การสร้างเครือข่ายความร่วมมือ เพื่อแบ่งปันข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า 2) การพัฒนาศักยภาพและเพิ่มทักษะบุคลากรด้านการรักษความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า - กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 3) การกำหนดขอบเขตการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า - กำหนดโครงสร้างและบทบาทหน้าที่การกำกับดูแลผู้ประกอบกิจการไฟฟ้าที่เข้าข่ายเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ - กำหนดหลักเกณฑ์การพิจารณาบริการที่สำคัญของภาคส่วนไฟฟ้าที่เหมาะสมและสอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี 4) การกำหนดแนวปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า - กำหนดแนวทางด้านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับภาคส่วนไฟฟ้า

หัวข้อ	รายละเอียด
	- กำหนดแนวทางด้านการตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับภาคส่วนไฟฟ้า - กำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ รวมถึงแผนรองรับเหตุวิกฤติที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับภาคส่วนไฟฟ้า - กำหนดแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของภาคส่วนไฟฟ้า - กำหนดแนวปฏิบัติที่ดีสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วนไฟฟ้า
9. ปัญหา/อุปสรรคในการดำเนินงาน	-
10. ตัวอย่างภาพถ่ายการดำเนินโครงการ	-
11. หน่วยงาน/ส่วนงานย่อยที่รับผิดชอบ	สำนักงานนโยบายและแผนพลังงาน / กลุ่มราคาไฟฟ้าและคุณภาพบริการ กองนโยบายไฟฟ้า