ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
และภารกิจหรือให้บริการที่เกี่ยวข้อง
พ.ศ. ๒๕๖๔

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าว ให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหมดหรือบางส่วนก็ได้ รวมถึงให้คณะกรรมการพิจารณากำหนดภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าว

อาศัยอำนาจตามความในมาตรา ๕๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในคราวการประชุมครั้งที่ ๑/๒๕๖๔ เมื่อวันที่ ๒๕ มิถุนายน ๒๕๖๔ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในแต่ละด้านจัดตั้งหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยหน่วยงานควบคุมหรือกำกับดูแลอาจจัดให้มีหลักเกณฑ์ เงื่อนไขและแนวทางในการพิจารณาคุณสมบัติ และความเหมาะสมของการเป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามวรรคหนึ่ง มีลักษณะ หน้าที่และความรับผิดชอบ รวมถึงจัดให้มีการดำเนินภารกิจหรือให้บริการไม่น้อยกว่าหลักเกณฑ์ที่กำหนดแนบท้ายประกาศฉบับนี้

ข้อ ๔ เมื่อมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านใดแล้ว ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านดังกล่าว พร้อมกับรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การดูแลและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบภายในสามสิบวันนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

ในกรณีที่มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพิ่มเติม หรือมีการเปลี่ยนแปลงใด ๆ เกี่ยวกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งเพิ่มเติมหรือการเปลี่ยนแปลงดังกล่าว พร้อมข้อมูลที่เกี่ยวข้อง ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบภายในสามสิบวันนับแต่วันที่จัดตั้งเพิ่มเติมหรือเปลี่ยนแปลงแล้วเสร็จ

ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรายงานการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามวรรคหนึ่งให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ โดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาจให้ข้อเสนอแนะหรือให้ความเห็นเพิ่มเติมได้

ข้อ ๕ ในระหว่างที่หน่วยงานของรัฐหน่วยงานใดยังไม่มีความพร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดังกล่าวแจ้งเหตุขัดข้อง หรือสาเหตุที่ทำให้ยังไม่มีความพร้อมให้หน่วยงานควบคุมหรือกำกับดูแลทราบ เพื่อให้หน่วยงานควบคุมหรือกำกับดูแลประสานงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อพิจารณาดำเนินการตามแนวทางที่เหมาะสม เพื่อให้การช่วยเหลือในด้านการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์แก่หน่วยงานดังกล่าว ต่อไป

ประกาศ ณ วันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๖๔
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔

คำนิยาม

๑.	ศูนย์ประสานการรักษาความมั่นคงปลอดภัย	หมายถึง	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒.	หน่วยงาน CII	หมายถึง	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) ที่อยู่ภายใต้การดูแลของศูนย์ประสานการรักษาความมั่นคงปลอดภัย
๓.	สำนักงาน	หมายถึง	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัย

๔. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจจัดตั้งขึ้นในลักษณะที่เป็นหน่วยงานอิสระที่มีการบริหารงานเป็นของตนเอง หรือกำหนดให้เป็นส่วนงานหนึ่งภายในองค์กรที่จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยหรือกำหนดให้เป็นหน่วยงานที่อยู่ภายใต้การดูแลของหน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแลซึ่งทำหน้าที่กำกับดูแลหน่วยงาน CII ในแต่ละด้าน หรืออาจจัดตั้งขึ้นในรูปแบบของการรวมกลุ่มระหว่างหน่วยงาน หรือผู้ประกอบธุรกิจที่มีภารกิจ หรือให้บริการในลักษณะเดียวกันหรือคล้ายคลึงกันก็ได้ ทั้งนี้ ให้หน่วยงานควบคุมหรือกำกับดูแลเป็นผู้แจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยตามแนวทางที่กำหนดในประกาศฉบับนี้

ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยที่จัดตั้งขึ้นนั้นมีหน้าที่และความรับผิดชอบในด้านการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ตลอดจนมีหน้าที่ในการช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

นอกจากนี้ ในการดำเนินการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยนั้น ควรมีการกำหนดภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยและบันทึกไว้เป็นลายลักษณ์อักษรในพันธกิจ (mission statement) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยดังกล่าว โดยพันธกิจนั้นจะต้องกำหนดวัตถุประสงค์และขอบเขตภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยให้ชัดเจนและต้องมีสาระสำคัญอย่างน้อย ดังต่อไปนี้

ภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัย

๕. ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยมีภารกิจหรือให้บริการที่เกี่ยวข้องกับการประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII เพื่อปกป้องหน่วยงานดังกล่าว ตลอดจนโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบงานที่มีความสำคัญอื่น ๆ จากภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อภารกิจหรือการให้บริการของหน่วยงาน CII โดยภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยนั้น สามารถแบ่งออกเป็น ๔ ด้าน ดังนี้

- ภารกิจหรือให้บริการในด้านการประสานงาน
- ภารกิจหรือให้บริการในด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์
- ภารกิจหรือให้บริการในด้านการรับมือและแก้ไขภัยคุกคามทางไซเบอร์
- ภารกิจหรือให้บริการในด้านการดำเนินมาตรการด้านการบริหารจัดการคุณภาพ

ทั้งนี้ ให้ภารกิจหรือให้บริการในแต่ละด้านของศูนย์ประสานการรักษาความมั่นคงปลอดภัย มีรายละเอียดอย่างน้อยดังต่อไปนี้ และในกรณีที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยใดมีความพร้อม อาจพิจารณาดำเนินภารกิจหรือจัดให้มีบริการเพิ่มเติมแก่หน่วยงาน CII โดยมีรายละเอียดปรากฏตามที่ระบุไว้ในภาคผนวก แนบท้ายนี้ทั้งหมดหรือบางส่วนก็ได้

ภารกิจหรือให้บริการในด้านการประสานงาน

๕.๑ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยประสานความร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการปฏิบัติหน้าที่ด้านการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ตลอดจนให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติในการดำเนินภารกิจหรือให้บริการ ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะการดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ การดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น และการดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น และควรให้ความสำคัญกับการแบ่งปันข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

นอกจากนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจร่วมมือกับหน่วยงานอื่น ๆ ที่ดำเนินภารกิจหรือให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ให้แก่หน่วยงานที่มีภารกิจหรือให้บริการในลักษณะเดียวกันหรือมีความเกี่ยวข้องกันกับหน่วยงาน CII เพื่อช่วยยกระดับความสามารถในการดำเนินภารกิจหรือให้บริการด้านต่าง ๆ ของศูนย์ประสานการรักษาความมั่นคงปลอดภัย ตลอดจนการปฏิบัติหน้าที่ในการเฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์

ภารกิจหรือให้บริการในด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์

๕.๒ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ให้แก่หน่วยงาน CII ดังต่อไปนี้

๕.๒.๑ เฝ้าระวังความเสี่ยงและติดตามแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงดำเนินการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงาน CII ดำเนินการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที

๕.๒.๒ วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้หน่วยงาน CII สามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่หน่วยงาน CII ในการตรวจจับเหตุการณ์ที่อาจนำมาสู่การบุกรุก และการวิเคราะห์ข้อมูล เป็นต้น

เพื่อประโยชน์ในการเฝ้าระวังและแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการเพื่อให้มีการรับลงทะเบียนข้อมูลและจัดทำบัญชีช่องทางการติดต่อ (point of contact) ของหน่วยงาน CII เพื่อใช้เป็นช่องทางหลักในการติดต่อสื่อสารระหว่างศูนย์ประสานการรักษาความมั่นคง

ปลอดภัยกับหน่วยงานดังกล่าว และจัดทำรายชื่อของหน่วยงาน CII รวมถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบงานที่มีความสำคัญอื่น ๆ ที่หน่วยงาน CII ใช้ในการดำเนินภารกิจหรือให้บริการในกิจการของตน ซึ่งจำเป็นต้องมีการเฝ้าระวัง หรือดำเนินการป้องกัน รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ และปรับปรุงข้อมูลดังกล่าว ให้เป็นปัจจุบันอยู่เสมอ

ภารกิจหรือให้บริการในด้านการรับมือและแก้ไขภัยคุกคามทางไซเบอร์

๕.๓ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแก่หน่วยงาน CII ดังต่อไปนี้

๕.๓.๑ เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ตลอดจนให้การสนับสนุนข้อมูลต่าง ๆ ที่จำเป็นต่อหน่วยงาน CII เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับและแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะหรือช่องทางอื่นใดตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยกำหนด

๕.๓.๒ ให้การช่วยเหลือ แนะนำ หรือสนับสนุนหน่วยงาน CII ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และปฏิบัติงานร่วมกับหน่วยงานควบคุมหรือกำกับดูแลในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ดังกล่าว

๕.๓.๓ เมื่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติแจ้งการเปลี่ยนแปลงระดับ หรือยกระดับการแจ้งเตือน หรือเมื่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยพบการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์หรือผลกระทบต่อภารกิจ หรือการให้บริการของหน่วยงาน CII ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยแจ้งการเปลี่ยนแปลง หรือดำเนินการแจ้งเตือนไปยังหน่วยงาน CII เพื่อให้หน่วยงานดังกล่าวเตรียมความพร้อมในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์

ในการดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ภารกิจหรือให้บริการในด้านการดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๔ ให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงาน CII ที่อยู่ภายใต้การดูแล โดยมีหน้าที่และความรับผิดชอบดังต่อไปนี้

๕.๔.๑ ผลักดันและสนับสนุนการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การดำเนินมาตรการในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๔.๒ ผลักดันและสนับสนุนการเพิ่มความรู้ความสามารถของหน่วยงาน CII เพื่อเตรียมความพร้อมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสามารถยกระดับการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และระบบงานที่มีความสำคัญอื่น ๆ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจดำเนินการจัดให้มีการฝึกอบรมและให้ความรู้แก่หน่วยงาน CII เพื่อสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Education Training and Awareness หรือ “ETA”) เช่น การวางแผนรับมือในสถานการณ์ที่ต้องเผชิญเหตุภัยคุกคามทางไซเบอร์หรือการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

การขอผ่อนผันภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัย

๖. ในระยะเริ่มต้นของการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัย หากศูนย์ประสานการรักษาความมั่นคงปลอดภัยในด้านใดยังไม่สามารถดำเนินภารกิจหรือให้บริการได้ครบถ้วนตามที่กำหนดแนบท้ายประกาศนี้ ให้หน่วยงานดังกล่าวหารือร่วมกับหน่วยงานควบคุมหรือกำกับดูแล เพื่อพิจารณากำหนดแนวทางการเริ่มต้นภารกิจหรือให้บริการของศูนย์ประสานการรักษาความมั่นคงปลอดภัย โดยอาจจัดทำแผนการปฏิบัติงานโดยแบ่งเป็นระยะต่าง ๆ ตามระดับความสำคัญและความพร้อมของหน่วยงาน และนำเสนอต่อสำนักงานเพื่อให้สำนักงานรายงานแผนการปฏิบัติงานดังกล่าวต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อพิจารณาต่อไป

ภาคผนวก
ภารกิจหรือให้บริการที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัย
อาจจัดให้มีเพิ่มเติมเพื่อให้บริการแก่หน่วยงาน CII ที่อยู่ภายใต้การดูแล

เมื่อมีความพร้อม ศูนย์ประสานการรักษาความมั่นคงปลอดภัยอาจพิจารณาดำเนินภารกิจหรือให้บริการเพิ่มเติมแก่หน่วยงาน CII ปรากฏตามรายละเอียดที่ระบุในภาคผนวกนี้ โดยอาจพิจารณาดำเนินการทั้งหมดหรือบางส่วนก็ได้

๑. จัดให้มีภารกิจหรือให้บริการเพิ่มเติมเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ เช่น

(ก) การจัดให้มีกลไกหรือกระบวนการทำงานที่เหมาะสมในการตรวจจับการเกิดภัยคุกคามทางไซเบอร์ หรืออาจใช้การวิเคราะห์ข้อมูลที่ได้รับจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ เพื่อเฝ้าระวังความเสี่ยงและประเมินแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

(ข) การติดตามความก้าวหน้าด้านเทคโนโลยีเพื่อจัดทำข้อเสนอแนะเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์หรือแนวปฏิบัติพื้นฐาน (baseline) ที่เกี่ยวข้องให้แก่หน่วยงาน CII เพื่อใช้เป็นแนวทางในการป้องกันหรือเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(ค) การให้ความช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินมาตรการป้องกันตามแนวทางปฏิบัติที่ดี (best practice) เพื่อให้หน่วยงาน CII สามารถเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(ง) การประเมินความเสี่ยงและช่องโหว่ที่อาจถูกใช้ในการก่อภัยคุกคามทางไซเบอร์เพื่อนำไปสู่การจัดการช่องโหว่ การดำเนินมาตรการป้องกัน หรือกระทำการอื่นใดเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการร้องขอจากหน่วยงาน CII

(จ) การดำเนินการอื่นใดที่เกี่ยวข้องเพื่อตรวจสอบโปรแกรม หรือค้นหาสิ่งที่ไม่พึงประสงค์ (malicious code) ซึ่งอาจเป็นอันตรายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ หรืออาจให้ความช่วยเหลือแก่หน่วยงาน CII ในการดำเนินการดังกล่าว เป็นต้น

๒. จัดให้มีภารกิจหรือให้บริการเพิ่มเติมเพื่อรับมือและแก้ไขภัยคุกคามทางไซเบอร์ เช่น

(ก) การให้ความช่วยเหลือ แนะนำ และสนับสนุนหน่วยงาน CII เกี่ยวกับวิธีการในการบรรเทาผลกระทบและแผนการฟื้นฟูเพื่อให้หน่วยงาน CII สามารถกลับมาดำเนินภารกิจหรือให้บริการได้ต่อไปภายหลังการระงับเหตุภัยคุกคามทางไซเบอร์เสร็จสิ้น

(ข) การให้ความช่วยเหลือ แนะนำ และสนับสนุนหน่วยงาน CII ในการดำเนินกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล การเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลต่าง ๆ ตลอดจนการสืบสวนหรือสอบสวนเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์ เป็นต้น

๓. จัดให้มีภารกิจหรือให้บริการเพิ่มเติมเพื่อดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น

(ก) ผลักดันและสนับสนุนหน่วยงาน CII ในการจัดทำแผนความต่อเนื่องของการดำเนินงาน (business continuity plan) เพื่อรับมือในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ แผนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (critical information infrastructure protection plan) และแผนฟื้นฟู (disaster recovery plan) ภายหลังเกิดภัยคุกคามทางไซเบอร์

(ข) ผลักดันและสนับสนุนหน่วยงาน CII ในการประเมินความเสี่ยงของการเกิดภัยคุกคามทางไซเบอร์ โดยอาจดำเนินการตรวจสอบความมั่นคงปลอดภัย (security assessments) ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ ด้วยวิธีการต่าง ๆ และให้คำแนะนำเพื่อยกระดับคุณภาพของการดำเนินมาตรการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความแข็งแกร่งมากขึ้น เป็นต้น
