รายงานผลการประเมินองค์การมหาชน
ประจำปีงบประมาณ พ.ศ. 2565

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ประจำปีงบประมาณ พ.ศ.2565

วัตถุประสงค์การจัดตั้ง	ข้อมูลพื้นฐาน
1. เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ 2. จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อ กกม. เพื่อให้ความเห็นชอบ 3. ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) 4. ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ 5. ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ 6. เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ 7. ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ 8. ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ 9. เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน 10. เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน 11. เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชนทั้งในประเทศและต่างประเทศ 12. ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ 13. ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ 14. ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ 15. รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ	**งบประมาณ** 404.2553 ล้านบาท **รายได้*** - ล้านบาท **เงินทุนสะสม** - ล้านบาท **อัตรากำลัง (กรอบ/บรรจุจริง)** 120/50 คน **ค่าใช้จ่ายบุคลากร** 40.0142 ล้านบาท **งบประมาณค่าใช้จ่ายตามแผนการใช้จ่ายเงิน (ประกอบด้วย เงินอุดหนุน+เงินทุนสะสม +รายได้)** 404.2553 ล้านบาท (ไม่รวมครุภัณฑ์) **สัดส่วนค่าใช้จ่ายด้านบุคลากร** ร้อยละ 9.89 **ข้อมูล ณ วันที่ 30 กันยายน 2565**

คณะกรรมการองค์การมหาชน			
		วันที่ได้รับแต่งตั้ง	**วันที่ครบวาระ**
ประธานกรรมการ	1. รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	-	-
กรรมการโดยตำแหน่ง	2. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	-	-
	3. อธิบดีกรมบัญชีกลาง	-	-
	4. เลขาธิการ ก.พ.	-	-
	5. เลขาธิการ ก.พ.ร	-	-
กรรมการผู้ทรงคุณวุฒิ	6. นายชัยชนะ มิตรพันธ์ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	20 ธ.ค.63	20 ธ.ค.67
	7. รองศาสตราจารย์สุรศักดิ์ สงวนพงษ์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	20 ธ.ค.63	20 ธ.ค.67
	8. รองศาสตราจารย์เสาวนีย์ ไทยรุ่งโรจน์ ด้านเศรษฐศาสตร์	20 ธ.ค.63	20 ธ.ค.67
	9. พลเอก ภุชพงศ์ พงษ์ศิริ ด้านสังคม	20 ธ.ค.63	20 ธ.ค.67
	10. นายสราวุธ เบจกุล ด้านกฎหมาย	20 ธ.ค.63	20 ธ.ค.67
	11. นางแก้วใจ นาคสกุล ด้านบริหารจัดการองค์กร	20 ธ.ค.63	20 ธ.ค.67
กรรมการและเลขานุการ (เลขาธิการ)	12. พลเอก ปรัชญา เฉลิมวัฒน์	1 ม.ค.64	30 ก.ย. 65

วิสัยทัศน์

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ

พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

แบบประเมินองค์การมหาชน ประจำปีงบประมาณ พ.ศ. 2565
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

ส่วนที่ 1 องค์ประกอบการประเมินผลการปฏิบัติงาน		ส่วนที่ 2 ตัวชี้วัดประกอบการประเมิน
สรุปผลการประเมินระดับองค์กร*	คะแนนรวมถ่วงน้ำหนัก	ITA**
ระดับดีมาก	91.83	-

ส่วนที่ 3 ตัวชี้วัดการติดตามผลกระทบเป็นรายปี (monitoring KPI)			
ตัวชี้วัด monitor	ค่าเป้าหมาย		
	2565	2566	2567
-	-	-	-
ผลการดำเนินงานปี 2565 : -			

หมายเหตุ :

* สรุปผลการประเมินระดับองค์กร

ระดับดีมาก หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 90 - 100 คะแนน

ระดับดี หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 75 – 89.99 คะแนน

ระดับพอใช้ หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 60 – 74.99 คะแนน

ระดับต้องปรับปรุง หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ต่ำกว่า 60 คะแนน

** ITA : Integrity and Transparency Assessment หรือ ระดับคุณธรรมและความโปร่งใสการดำเนินงานของหน่วยงาน ประเมินโดย สำนักงาน ป.ป.ช.

1

ส่วนที่ 1 องค์ประกอบการประเมินผลการปฏิบัติงาน

ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
		เป้าหมายขั้นต่ำ (50)	เป้าหมายมาตรฐาน (75)	เป้าหมายขั้นสูง (100)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่าเป้าหมาย)	คะแนนถ่วงน้ำหนัก
Performance Perspective							
องค์ประกอบที่ 1 ประสิทธิผลการดำเนินงาน (ร้อยละ 40)							
1.1 ตัวชีวัดที่สอดคล้องกับภารกิจตามวัตถุประสงค์การจัดตั้งที่แสดงให้เห็นการเชื่อมโยงยุทธศาสตร์ชาติ นโยบายระดับชาติ							
1.1.1 ความสำเร็จของการจัดทำนโยบาย/แผน/กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐานที่สนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	5	4 เรื่องและดำเนินการได้ตามแผนปฏิบัติการ 3 ปี สกมช. ร้อยละ 40	5 เรื่องและดำเนินการได้ตามแผนปฏิบัติการ3 ปี สกมช. ร้อยละ 50	6 เรื่องและดำเนินการได้ตามแผนปฏิบัติการ 3 ปี สกมช. ร้อยละ 60	มีการจัดทำนโยบาย/แผน จำนวน 6 เรื่อง	100	5
1.1.2 ร้อยความสำเร็จการจัดตั้งศูนย์ประสานการรักษาความมั่งคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100	100	4
1.1.3 ร้อยละความสำเร็จการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Lab)	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100	100	4
1.1.4 ร้อยละความสำเร็จในการทำระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100	100	4
1.1.5 ร้อยละความสำเร็จในการจัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)	4	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100	100	4
1.1.6 ความสำเร็จด้านความร่วมมือระหว่างประเทศ	1	40 ครั้ง	60 ครั้ง	80 ครั้ง	95 ครั้ง	100	1
1.1.7 ความสำเร็จด้านการเผยแพร่ประชาสัมพันธ์ และสร้างความตระหนักรู้ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	2	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 100	100	2
1.1.8 ความสำเร็จการประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์ของประเทศ	3	ร้อยละ 70	ร้อยละ 85	ร้อยละ 100	ร้อยละ 90	79.41	2.38
1.1.9 ความสำเร็จการจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	3	100 คน	150 คน	150 คน พร้อมมีรายงานการจัดทำสถานการณ์ฝึก	418 คน พร้อมมีรายงานการจัดทำสถานการณ์ฝึก	100	3

ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
		เป้าหมายขั้นต่ำ (50)	เป้าหมายมาตรฐาน (75)	เป้าหมายขั้นสูง (100)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่าเป้าหมาย)	คะแนนถ่วงน้ำหนัก
1.2 ตัวชีวัดทีสอดคล้องกับนโยบายสำคัญหรือแผนปฏิบัติการของกระทรวงทีมุ่งเน้นการขับเคลือนการบูรณาการร่วมกันระหว่างหน่วยงานภายในกระทรวงเพือบรรลุเป้าหมายร่วมกัน							
1.2.1 ความสำเร็จการดำเนินการโครงการการยกระดับทักษะบุคลากรภาครัฐเพื่อตอบโจทย์ความต้องการของประเทศ กิจกรรม พัฒนาขีดความสามารถผู้ปฏิบัติงานตามมาตรฐานสากล	10	จำนวนผู้ได้รับการพัฒนา 300 คน และผู้ได้รับการพัฒนาผ่านเกณฑ์การระเมินไม่น้อยกว่าร้อยละ 60	จำนวนผู้ได้รับการพัฒนา 350 คน และผู้ได้รับการพัฒนาผ่านเกณฑ์การประเมินไม่น้อยกว่าร้อยละ 70	จำนวนผู้ได้รับการพัฒนา 400 คน และผู้ได้รับการพัฒนาผ่านเกณฑ์การประเมินไม่น้อยกว่าร้อยละ 80	จำนวนผู้ได้รับการพัฒนา 451 คน และผู้ได้รับการพัฒนาผ่านเกณฑ์การประเมินร้อยละ 93.56	100	10
องค์ประกอบที่ 2 ประสิทธิภาพและความคุ้มค่าในการดำเนินงาน (ร้อยละ 30)							
2.1.1 โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive Cybersecurity Capacity Building Program) ระยะที่ 1	20	จำนวนบุคลากรด้านการรักษาความมนคงปลอดภัยไซเบอร์ได้รับการพัฒนาศักยภาพ 1,500 คน	จำนวนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาศักยภาพ 2,000 คน	จำนวนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาศักยภาพ 2,000 คน และสอบผ่านเกณฑ์ไม่น้อยกว่าร้อยละ 50	จำนวนบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาศักยภาพ 2,335 คน และสอบผ่านเกณฑ์ร้อยละ 68.7	100	20
2.2.1 ความสำเร็จการสำรวจความพร้อมด้าน IT ดิจิทัล และความมั่นคงปลอดภัยไซเบอร์	5	ศึกษาวิเคราะห์และดำเนินการสำรวจความพร้อมด้าน IT ดิจิทัล และความมั่นคงปลอดภัยไซเบอร์	มีรายงานสรุปผลความพร้อมด้าน IT ดิจิทัล และความมั่นคงปลอดภัยไซเบอร์เสนอผู้บริหารหน่วยงาน	มีรายงานสรุปผลความพร้อมด้าน IT ดิจิทัล และความมั่นคงปลอดภัยไซเบอร์เสนอต่อ กบส. และ/หรือ กมช.	มีรายงานสรุปผลความพร้อมด้าน IT ดิจิทัลและความมั่นคงปลอดภัยไซเบอร์รายงานต่อ เลขาธิการ ตามเอกสารที่ สกมช. 0500/23	75	3.75
2.2 ร้อยละค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน	5	-	-	ไม่เกินร้อยละ 30 ของแผนการใช้จ่ายเงินประจำปีตามมติ ครม. ในการประชุมวันที่ 28 พฤษภาคม 2561	คำนวณได้ 9.89	100	5

ตัวชี้วัด	น้ำหนัก (ร้อยละ)	เกณฑ์การประเมิน			ผลการดำเนินงาน		
		เป้าหมายขั้นต่ำ (50)	เป้าหมายมาตรฐาน (75)	เป้าหมายขั้นสูง (100)	ผลการดำเนินงาน	คะแนนที่ได้ (เทียบจากค่าเป้าหมาย)	คะแนนถ่วงน้ำหนัก
Potential Perspective							
องค์ประกอบที่ 3 ศักยภาพขององค์การมหาชน (ร้อยละ 20)							
3.1 ผลการพัฒนาศักยภาพองค์การสู่การเป็นระบบราชการ 4.0							
3.1.1 การพัฒนาองค์การสู่ดิจิทัล 1) การพัฒนาระบบบัญชีข้อมูล (Data Catalog) เพื่อนำไปสู่การเปิดเผยข้อมูลภาครัฐ (Open Data)	10	มีรายชื่อชุดข้อมูล (Data Set) ที่สัมพันธ์กับ Focus Area	มีคำอธิบายข้อมูล (Meta Data) 14 รายการทุกชุดข้อมูลและมีระบบบัญชีข้อมูลหน่วยงานพร้อมแจ้ง URL	มีการประเมินคุณภาพชุดข้อมูลและการนำข้อมูลไปใช้ประโยชน์	จากผลการประเมินโดยสำนักงาน ก.พ.ร. ได้คะแนน 75 คะแนน	75	7.5
3.1.2 การประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)	10	10	มี (ร่าง) ผลการประเมินตามแนวทางของ PMQA 4.0	ส่งผลการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)	ได้คะแนน >350 คะแนน	ส่งผลการประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0) ไปแล้วแต่ได้ 210 คะแนน (บันทึกข้อความที่ สกมช 0013/13)	75
องค์ประกอบที่ 4 การควบคุมดูแลกิจการขององคณะกรรมการองค์การมหาชน (ร้อยละ 10)							
4.1 ร้อยละความสำเร็จของการพัฒนาด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน	15	ร้อยละ 100			ร้อยละ 87	87	8.7
						คะแนนรวม	**91.83**
						สรุปผลการประเมินระดับองค์กร	

สรุปผลการประเมินระดับองค์กร

ระดับดีมาก หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 90 - 100 คะแนน
ระดับดี หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 75 – 89.99 คะแนน
ระดับพอใช้ หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ตั้งแต่ 60 – 74.99 คะแนน
ระดับต้องปรับปรุง หมายถึง องค์การมหาชนที่มีผลคะแนนเฉลี่ยทุกองค์ประกอบ ต่ำกว่า 60 คะแนน

ผลการดำเนินงานตามตัวชี้วัดการติดตามผลกระทบเป็นรายปี (monitoring KPI)

ตัวชี้วัด	ปี 2564		ปี 2565		ปี 2566	ปี 2567
	เป้าหมาย	ผลการดำเนินงาน	เป้าหมาย	ผลการดำเนินงาน	เป้าหมาย	เป้าหมาย
1.						
2.						

สรุปผลงานสำคัญ ปีงบประมาณ พ.ศ. 2565

- มีการจัดทำนโยบาย / แผน/กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐานที่สนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศที่ กกม. และ กมช.
- พิจารณาให้ความเห็นชอบ จำนวน 6 เรื่อง
- มีการฝึกอบรมขีดความสามารถทางไซเบอร์ระดับประเทศ พร้อมหนังสือคู่มือการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ THAILAND'S NATIONAL CYBER EXERCISE 2022 เพื่อเตรียมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วนงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง มีความรู้ความเข้าใจเพิ่มมากขึ้นเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- มี (ร่าง) แนวทางการประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์ของประเทศจำนวน 3 ฉบับ
    - (ร่าง) ประกาศ กรอบการบริหารความเสี่ยงด้านไซเบอร์ (NIST SP 800-3) เรื่องกรอบการบริหารความเสี่ยงด้านไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
    - (ร่าง) ประกาศ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (NIST SP 800-39) เรื่อง การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
    - (ร่าง) ประกาศ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST SP 800-30) เรื่องการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
- มี (ร่าง) แนวทางการประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์ของประเทศจำนวน 3 ฉบับ
    - (ร่าง) ประกาศ กรอบการบริหารความเสี่ยงด้านไซเบอร์ (NIST SP 800-3) เรื่องกรอบการบริหารความเสี่ยงด้านไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
    - (ร่าง) ประกาศ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (NIST SP 800-39) เรื่อง การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
    - (ร่าง) ประกาศ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST SP 800-30) เรื่องการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
- มีการจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) และเสนอในการประชุม ครม. เมื่อวันที่ 20 กันยายน 2565 มีมติเห็นชอบ (ร่าง) นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)