สำนักนายกรัฐมนตรี
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เอกสารประกอบการชี้แจง

เสนอ

คณะกรรมาธิการวิสามัญพิจารณาศึกษา
ร่างพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ
พ.ศ. 2569
วุฒิสภา

เอกสารประกอบการชี้แจง

สำนักการเงินและกลยุทธ์องค์กร

สารบัญ

		หน้า
1.	รายนามผู้ชี้แจง	1
2.	วิสัยทัศน์ พันธกิจ โครงสร้างหน่วยงาน การดำเนินภารกิจหน้าที่และอำนาจตามกฎหมายจัดตั้งหน่วยงาน และการบูรณาการหรือประสานภารกิจในมติด้านอื่น	2 - 6
3.	ภาพรวมงบประมาณของหน่วยรับงบประมาณ 3 ปีย้อนหลัง (ปีงบประมาณ พ.ศ. 2567-2569) **ตามแบบ สว.69-01 (กรม/หน่วยงาน)**	7 - 9
4.	ภาพรวมแผนงาน ผลผลิต/โครงการ และโครงการที่สำคัญ ประจำปีงบประมาณ พ.ศ. 2569 **ตามแบบ สว.69-02 (กรม/หน่วยงาน)**	10 - 17
5.	ผลการเบิกจ่ายและผลการดำเนินงานในปีงบประมาณ พ.ศ. 2567-2568 **ตามแบบ สว.69-03 (กรม/หน่วยงาน)**	18 - 30
6.	การดำเนินการตามข้อสังเกตของคณะกรรมาธิการวิสามัญพิจารณาศึกษาร่างพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2568 วุฒิสภา **ตามแบบ สว.69-04 (กรม/หน่วยงาน)**	31 - 38

1. รายนามผู้ชี้แจง
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ลำดับ	ชื่อ - สกุล	ตำแหน่ง
1.	พลอากาศตรี อมร ชมเชย	เลขาธิการ
2.	พลตรี ธีรวุฒิ วิทยากรณ์	รองเลขาธิการ
3.	นายจิรศักดิ์ วิชัยกุล	ผู้ทรงคุณวุฒิพิเศษ
4.	นาวาอากาศเอก ธวัชชัย มากพานิช	ผู้อำนวยการ
5.	นาวาอากาศตรี กิตติ บวรพศวัตกิตติ์	ผู้อำนวยการฝ่าย

ผู้ประสานงาน

1.	นางสาววรรณวิสา เหล่าแช่ม	เจ้าหน้าที่ 095-7563214
2.	นางสาวชมพูนุท กันเขียว	เจ้าหน้าที่ 090-9109802

2. วิสัยทัศน์ พันธกิจ โครงสร้างหน่วยงาน การดำเนินภารกิจหน้าที่และอำนาจ ตามกฎหมายจัดตั้งหน่วยงาน และการบูรณาการหรือประสานภารกิจในมิติด้านอื่น

2. วิสัยทัศน์ พันธกิจ โครงสร้างหน่วยงาน การดำเนินภารกิจหน้าที่และอำนาจ ตามกฎหมายจัดตั้งหน่วยงาน และการบูรณาการหรือประสานภารกิจในมิติด้านอื่น

<u>วิสัยทัศน์</u>

เป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามไซเบอร์ทุกมิติ

<u>พันธกิจ</u>

1. เสนอแนะนโยบายแผนยุทธศาสตร์และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งศึกษาวิจัยกำหนดแนวทางมาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

2. กำกับดูแลเฝ้าระวัง ติดตาม วิเคราะห์ ประมวลผล แจ้งเตือน และปฏิบัติการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

3. เป็นศูนย์กลางในการประสานความร่วมมือรวมทั้ง ส่งเสริม สนับสนุน และช่วยเหลือหน่วยงานภาครัฐและเอกชนทั้งในประเทศและต่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

4. เผยแพร่ความรู้ความเข้าใจและสนับสนุนการพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

<u>ภารกิจ</u>

1. เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 9 ต่อคณะกรรมการ

2. จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 13 วรรคหนึ่ง (4) เสนอต่อ กกม. เพื่อให้ความเห็นชอบ

3. ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 53 และมาตรา 54

4. ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

5. ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

6. เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

7. ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือตามคำสั่งของคณะกรรมการ

8. ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

9. เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

10. เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

11. เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

12. ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

13. ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

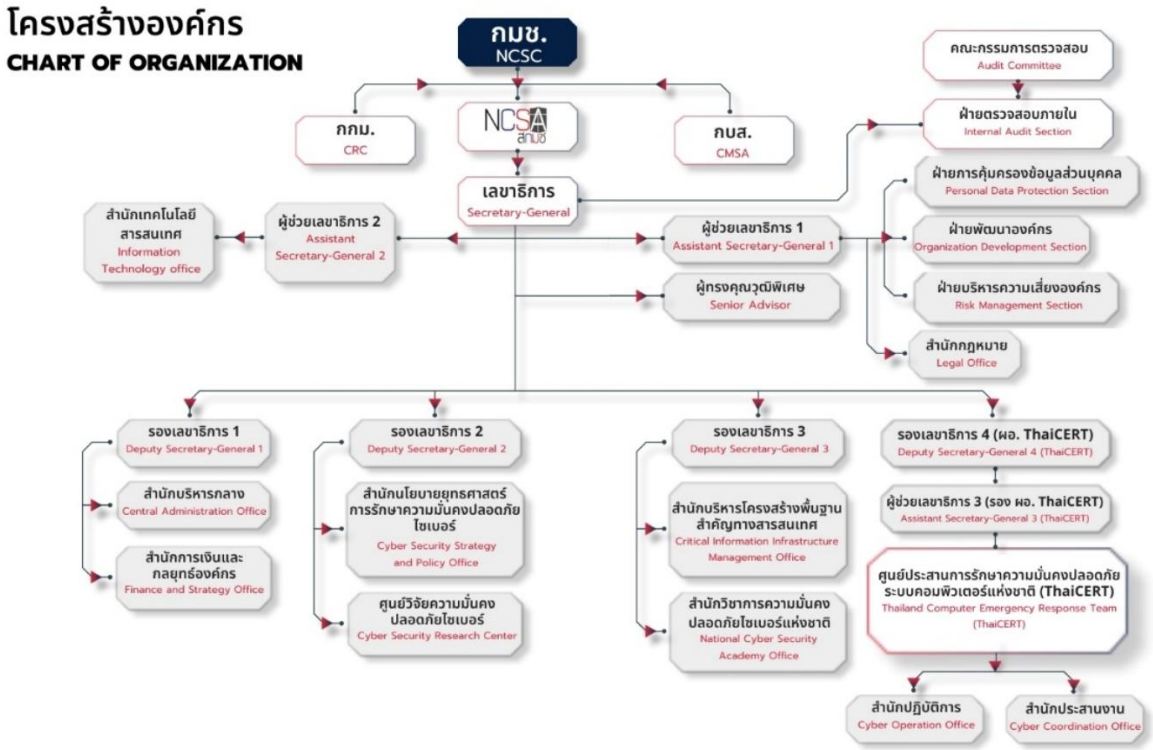
14. ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

15. รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ ทั้งนี้ ตามระยะเวลาที่คณะกรรมการกำหนด

16. ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

ทั้งนี้ เพื่อประโยชน์ในการดำเนินการตามหน้าที่และอำนาจตามข้อ 6 ให้สำนักงานจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงาน ให้มีหน้าที่และอำนาจตามที่คณะกรรมการกำหนด

โครงสร้างหน่วยงาน



โครงสร้างอัตรากำลังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กนช.	15	
กกม.	19	
กกส.	12	
เลขาธิการ	1	1
คณะกรรมการตรวจสอบ		
ฝ่ายตรวจสอบภายใน	3	2
รองเลขาธิการ 1	1	
รองเลขาธิการ 2	1	
รองเลขาธิการ 3	1	
รองเลขาธิการ 4 ผอ.ศูนย์ฯ	1	1
ผู้ตรวจกฎหมาย 1	1	1
ผู้ตรวจกฎหมาย 2	1	1
ผู้ช่วยเลขาธิการ 1	1	1
ผู้ช่วยเลขาธิการ 2	1	1
ผู้ช่วยเลขาธิการ 3 รอง ผอ.ศูนย์ฯ	1	1

สำนักเลขาธิการสนเทศ	22	6
ผอ. 1		ผรช. 1
ฝ่ายระบบคอมพิวเตอร์และเครือข่าย	7	1
ฝ่ายระบบสารสนเทศ	7	4
ฝ่ายบริหารความมั่นคงปลอดภัย	6	1

สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	60	12
ผอ. 1		ผรช. 2
ฝ่ายนโยบายและแผน	18	
ผู้อำนวยการฝ่าย	1	
งานนโยบายและแผน	9	
งานพัฒนากฎหมาย	8	1
ศูนย์ความเป็นเลิศ	18	
ผู้อำนวยการฝ่าย	1	1
งานประสานความร่วมมือ	9	
งานบริการวิชาการ	8	1
ฝ่ายบริหารการศึกษา	18	
ผู้อำนวยการฝ่าย	1	1
งานจัดการศึกษา	9	2
งานสนับสนุนการศึกษา	8	6
งานสารบรรณและธุรการ	3	

สำนักการเงินและกลยุทธ์องค์กร	31	9
ผอ. 1		ผรช. 1
ฝ่ายการเงินและบัญชี	9	
ผู้อำนวยการฝ่าย	1	1
งานการเงิน	5	2
งานบัญชี	3	1
ฝ่ายงบประมาณและจัดหารายได้	10	
ผู้อำนวยการฝ่าย	1	1
งานงบประมาณ	3	1
งานจัดหารายได้	3	
งานติดตามและประเมินผล	3	
ฝ่ายพัสดุ	10	
ผู้อำนวยการฝ่าย	1	
งานจัดซื้อจัดจ้างและบริหารสัญญา	6	
งานการบริหารพัสดุ	3	3
ฝ่ายบริหารความเสี่ยงองค์กร	3	1

สำนักนโยบายยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์	45	11
ผอ. 1	1	ผรช. 1	1
ฝ่ายนโยบายยุทธศาสตร์	10	
ผู้อำนวยการฝ่าย	1	1
งานยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซ	5	
งานยุทธศาสตร์องค์กร	4	1
ฝ่ายขับเคลื่อนยุทธศาสตร์ประเทศ	10	
ผู้อำนวยการฝ่าย	1	1
งานขับเคลื่อนยุทธศาสตร์ประเทศ	4	1
งานขับเคลื่อนนโยบายและแผนประเทศ	5	1
ฝ่ายยุทธศาสตร์ความร่วมมือในประเทศ	10	
ผู้อำนวยการฝ่าย	1	
งานยุทธศาสตร์การจัดทำความร่วมมือ	4	1
งานยุทธศาสตร์การบริหารความร่วมมือ	5	
ฝ่ายยุทธศาสตร์ความร่วมมือระหว่างประเทศ	10	
ผู้อำนวยการฝ่าย	1	1
งานยุทธศาสตร์ความร่วมมือทวิภาคี	4	1
งานยุทธศาสตร์ความร่วมมือพหุภาคี	5	
ฝ่ายพัฒนาองค์กร	3	1

ศูนย์ใช้ร่วมความมั่นคงปลอดภัยไซเบอร์	44	9
ผอ. 1	1	ผรช. 1
ฝ่ายวิจัยและเครือข่ายการวิจัย	13	
ผู้อำนวยการฝ่าย	1	1
งานวิจัย	6	1
งานพัฒนาเครือข่ายวิจัย	6	1
ฝ่ายฐานข้อมูลความรู้	7	
ฝ่ายวิเคราะห์และประมวลผลข้อมูล	7	2
ฝ่ายทดสอบและรับรอง	12	
ผู้อำนวยการฝ่าย	1	1
งานวิเคราะห์และทดสอบ	6	
งานรับรองมาตรฐาน	5	2
งานสารบรรณและธุรการ	3	1

สำนักบริหารกลาง	46	20
ผอ. 1	1	ผรช. 1	1
ฝ่ายอำนวยการ	21	
ผู้อำนวยการฝ่าย	1	
งานสรรหาบุคลากร	7	4
งานสวรรคและธุรการ	4	4
งานสาธารณและอาคารสถถน	4	2
งานพิธีการและการประชุม	5	1
ฝ่ายทรัพยากรบุคคล	13	
ผู้อำนวยการฝ่าย	1	1
งานสรรหาบุคลากร	4	1
งานบริหารทรัพยากรบุคคล	4	1
งานพัฒนาทรัพยากรบุคคล	4	1
ฝ่ายสื่อสารองค์กร	10	
ผู้อำนวยการฝ่าย	1	
งานประชาสัมพันธ์	5	3
งานกิจกรรมสัมพันธ์	4	

สำนักกฎหมาย	20	6
ผอ. 1	1	ผรช. 1	
ฝ่ายกฎหมายและระเบียบ	6	3
ฝ่ายนิติกรรมและสัญญา	4	1
ฝ่ายไม้ป	4	
ฝ่ายคดี	5	1
ฝ่ายสืบหรือข้อมูลส่วนบุคคล	3	1

สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	61	12
ผอ. 1	1	ผรช. 2
ฝ่ายกำหนดมาตรฐาน	13	
ผู้อำนวยการฝ่าย	1	1
งานประเมินและทางปฏิบัติและกระบะมาตรฐาน	6	1
งานกำหนดมาตรฐาน	6	1
ฝ่ายตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์	16	
ผู้อำนวยการฝ่าย	1	1
งานตรวจสอบที่ 1	5	1
งานตรวจสอบที่ 2	5	1
งานตรวจสอบที่ 3	5	1
ฝ่ายทดสอบเจาะระบบและประเมินความพร้อม	13	
ผู้อำนวยการฝ่าย	1	1
งานทดสอบเจาะระบบ	6	
งานประเมินความพร้อม	6	
ฝ่ายเฝ้าข้อมูลและทดสอบสถานความพร้อม	13	
ผู้อำนวยการฝ่าย	1	1
งานบางผลผลประเมินการฝึก	6	
งานสารบรรณและธุรการ	3	2

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	129	24
สำนักประสานงาน	61	11
ผอ. 1	1	ผรช. 2
ฝ่ายประสานงานภาครัฐและกรอบ	16	
ผู้อำนวยการฝ่าย	1	
งานประสานงานการแจ้งเตือนภัยทุกทางไซเบ	5	3
งานความร่วมมือภาครัฐและเอกชน	5	2
งานประชาคมไซเบอร์	5	
ฝ่ายประสานงานกิจการต่างประเทศ	12	
ผู้อำนวยการฝ่าย	1	
งานผลผลานและโครงการ	5	
งานความร่วมมือต่างประเทศ	6	1
ฝ่ายประสานความช่วยเหลือ	16	
ผู้อำนวยการฝ่าย	1	
งานประสานความช่วยเหลือ 1	5	1
งานประสานความช่วยเหลือ 2	5	
งานประสานความช่วยเหลือ 3	5	
ผู้อำนวยการฝ่าย	1	1
งานศูนย์ข้อมูลภัยคุกคามทางไซเบอร์	5	
งานซีทีไอทุกคามทางไซเบอร์	5	
งานสารบรรณและธุรการ	3	2

สำนักปฏิบัติการ	68	13
ผอ. 1		ผรช. 2
ฝ่ายแก้ไขความมั่นคงปลอดภัยทางไซเบอร์	24	
ผู้อำนวยการฝ่าย	1	1
งานแก้ไขวิบัติทุกคามทางไซเบอร์	14	
งานวิเคราะห์ภัยทุกคามทางไซเบอร์	9	2
ฝ่ายปฏิบัติการทางไซเบอร์	20	
ผู้อำนวยการฝ่าย	1	
งานข่ายตรวจทางไซเบอร์	7	1
งานประเมินภัยคุกคามทางไซเบอร์	6	3
งานปฏิบัติการทางไซเบอร์	6	2
ฝ่ายตอบสนองและรับมือภัยคุกคามทางไซเบอร์	10	
ผู้อำนวยการฝ่าย	1	
งานตอบสนองและรับมือ 1	4	
งานตอบสนองและรับมือ 2	5	
ฝ่ายสืบสวนและตรวจพิสูจน์นิติธุรกรรมทางไซเบอร์	8	
งานสืบสวนพิทางไซเบอร์	3	1
งานตรวจพิสูจน์ทางดิจิทัล	4	1
งานสารบรรณและธุรการ	3	1

เลขาธิการ	1	1
รองเลขาธิการ	4	1
ผู้ตรวจกฎหมาย	2	2
ผู้ช่วยเลขาธิการ	3	3
ผู้อำนวยการสำนัก	10	6
ผู้เชี่ยวชาญพิเศษ	14	2
ฝ่ายขึ้นตรงกับเลขาธิการ	12	5
พนักงาน	434	101
รวมทั้งสิ้น	480	121

ข้อมูล ณ วันที่ 30 เม.ย. 68

3. ภาพรวมงบประมาณของหน่วยรับงบประมาณ 3 ปีย้อนหลัง
(ปีงบประมาณ พ.ศ. 2567-2569)

(แบบ สว.69-01 (กรม/หน่วยงาน))

ภาพรวมงบประมาณของหน่วยรับงบประมาณ 3 ปีย้อนหลัง
(ปีงบประมาณ พ.ศ. 2567-2569)

.....

ชื่อหน่วยงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1. จำแนกตามลักษณะรายจ่าย

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

รายการ	ปี 2567 (1)	ปี 2568 (2)	ปี 2569 (3)	เปรียบเทียบ (2) และ (3)	
				เพิ่มขึ้น/ลดลง	ร้อยละ
รวมทั้งสิ้น	**487.0914**	**486.1870**	**547.3586**	**61.1716**	**12.58**
1.1 รายจ่ายประจำ	175.0097	227.1695	249.0342	21.8647	9.62
1.2 รายจ่ายลงทุน	312.0817	259.0175	298.3244	39.3069	15.18

2. จำแนกตามงบรายจ่าย

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

รายการ	ปี 2567 (1)	ปี 2568 (2)	ปี 2569 (3)	เปรียบเทียบ (2) และ (3)	
				เพิ่มขึ้น/ลดลง	ร้อยละ
รวมทั้งสิ้น	**487.0914**	**486.1870**	**547.3586**	**61.1716**	**12.58**
2.1 งบบุคลากร					
2.2 งบดำเนินงาน					
2.3 งบลงทุน					
2.4 งบเงินอุดหนุน	487.0914	486.1870	547.3586	61.1716	12.58
2.5 งบรายจ่ายอื่น					

3. เงินนอกงบประมาณของหน่วยรับงบประมาณ

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

รายการ	ปี 2567 (1)	ปี 2568 (2)	ปี 2569 (3)	เปรียบเทียบ (2) และ (3)	
				เพิ่มขึ้น/ลดลง	ร้อยละ
3.1 เงินนอกงบประมาณสะสมคงเหลือยกมา	319.4677				
3.2 รายได้ประเภทเงินนอกงบประมาณ	405.6852	250.4079		(250.4079)	(100)
3.3 รวมเงินนอกงบประมาณทั้งสิ้น (3.1+3.2)	**725.1529**	**250.4079**		(250.4079)	(100)
3.4 นำไปสมทบกับงบประมาณ					
(1) งบบุคลากร					
(2) งบดำเนินงาน					
(3) งบลงทุน					
(4) งบเงินอุดหนุน					
(5) งบรายจ่ายอื่น					
3.5 คงเหลือหลังหักเงินนำไปสมทบกับงบประมาณ (3.3-3.4)	**725.1529**	**250.4079**		(250.4079)	(100)

รายการ	ปี 2567 (1)	ปี 2568 (2)	ปี 2569 (3)	เปรียบเทียบ (2) และ (3)	
				เพิ่มขึ้น/ลดลง	ร้อยละ
3.6 แผนการใช้จ่ายอื่น	**725.1529**	**250.4079**		**(250.4079)**	**(100)**
(1) ภารกิจพื้นฐาน					
- รายจ่ายประจำ					
- รายจ่ายลงทุน					
(2) ภารกิจเพื่อการพัฒนา	725.1529	250.4079		(250.4079)	(100)
- รายจ่ายประจำ	725.1529	236.7699		(236.7699)	(100)
- รายจ่ายลงทุน		13.6380		(13.6380)	(100)
3.7 คงเหลือ (3.5-3.6)					

หมายเหตุ : วงเงินที่นำไปสมทบตามแนวทางการจัดทำงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2569 ตามฐานข้อมูลสำนักงบประมาณ และ/หรือ เอกสารงบประมาณ

4. งบประมาณตามยุทธศาสตร์การจัดสรรงบประมาณ จำแนกตามกลุ่มแผนงาน 3 ปีย้อนหลัง

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

ประเภทงบประมาณรายจ่าย - แผนงาน		ปี 2567 (1)	ปี 2568 (2)	ปี 2569 (3)	เปรียบเทียบ (2) และ (3)	
					เพิ่มขึ้น/(ลดลง)	ร้อยละ
รวมทั้งสิ้น		**487.0914**	**486.1870**	**547.3586**	**61.1716**	**12.58**
4.1	**แผนงานพื้นฐาน**					
	(1) แผนงานพื้นฐานด้าน					
	(2) แผนงานพื้นฐานด้าน					
4.2	**แผนงานยุทธศาสตร์**	**309.6302**	**319.2091**	**298.0500**	**(21.1591)**	**(6.63)**
	แผนงานยุทธศาสตร์ป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง	309.6302	319.2091	298.0500	(21.1591)	(6.63)
4.3	**แผนงานบูรณาการ**	**119.4456**	**97.3393**	**149.8546**	**52.5153**	**53.95**
	แผนงานบูรณาการรัฐบาลดิจิทัล	119.4456	97.3393	149.8546	52.5153	53.95
4.4	**แผนงานบุคลากรภาครัฐ**	**58.0156**	**69.6386**	**99.4540**	**29.8154**	**42.81**
4.5	**รายการค่าดำเนินการภาครัฐ**					

4. ภาพรวมแผนงาน ผลผลิต/โครงการ และโครงการที่สำคัญ ประจำปีงบประมาณ พ.ศ. 2569

(แบบ สว.69-02 (กรม/หน่วยงาน))

ภาพรวมแผนงาน ผลผลิต/โครงการ และโครงการที่สำคัญ
ประจำปีงบประมาณ พ.ศ. 2569

.....

ชื่อหน่วยงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1 ภาพรวมแผนงาน ผลผลิต/โครงการ จำแนกตามงบรายจ่าย

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

แผนงาน – ผลผลิต/โครงการ (ทุกแผนงาน)	งบบุคลากร					งบดำเนินงาน					งบลงทุน			งบอุดหนุน	งบรายจ่ายอื่น	รวมทั้งสิ้น
	เงินเดือน	ค่าจ้างประจำ	ค่าจ้างชั่วคราว	ค่าตอบแทนพนักงานฯ	รวม	ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าสาธารณูปโภค	รวม	ค่าครุภัณฑ์	ที่ดินและสิ่งก่อสร้าง	รวม			
1. แผนงานยุทธศาสตร์ แผนงานยุทธศาสตร์ป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง														**298.0500**		**298.0500**
ผลผลิตที่ 1 : ส่งเสริมการบริหารงานด้านความมั่นคงปลอดภัยไซเบอร์														11.6632		11.6632
โครงการที่ 2 : โครงการบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์														2.2685		2.2685
โครงการที่ 3 : โครงการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐานสากล														185.8466		185.8466
โครงการที่ 4 : โครงการเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ														94.5917		94.5917
โครงการที่ 5 : โครงการส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้														3.6800		3.6800

แผนงาน – ผลผลิต/โครงการ (ทุกแผนงาน)	งบบุคลากร					งบดำเนินงาน					งบลงทุน			งบอุดหนุน	งบรายจ่ายอื่น	รวมทั้งสิ้น
	เงินเดือน	ค่าจ้างประจำ	ค่าจ้างชั่วคราว	ค่าตอบแทนพนักงานฯ	รวม	ค่าตอบแทน	ค่าใช้สอย	ค่าวัสดุ	ค่าสาธารณูปโภค	รวม	ค่าครุภัณฑ์	ที่ดินและสิ่งก่อสร้าง	รวม			
2. แผนงานบูรณาการรัฐบาลดิจิทัล														**149.8546**		**149.8546**
โครงการที่ 1 : โครงการพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์														149.8546		149.8546
3. แผนงานบุคลากรภาครัฐ														**99.4540**		**99.4540**

คำชี้แจง : 1. ให้กรม/หน่วยงาน ระบุข้อมูลทุกแผนงานที่ได้รับจัดสรรงบประมาณ

2. ให้ระบุข้อมูลเฉพาะผลผลิต/โครงการ ที่อยู่ในแผน ทุกโครงการ โดย**ไม่ต้องลงรายละเอียดถึงกิจกรรม**

3. เฉพาะ **"แผนงานพื้นฐาน" และ "แผนงานบุคลากรภาครัฐ" ให้ระบุเฉพาะภาพรวมตัวเลขงบประมาณ** ไม่ต้องระบุรายละเอียด ผลผลิต/โครงการ กิจกรรม

4. ใช้ฐานข้อมูลตามคำของบประมาณ **แบบ สงป.1009 (หน่วยงาน)** : คู่มือปฏิบัติการจัดทำคำของบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2569 และ/หรือ เอกสารงบประมาณเล่มขาวคาดแดง

2. โครงการที่สำคัญ ประจำปีงบประมาณ พ.ศ. 2569

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

แผนงาน – ผลผลิต/โครงการ – กิจกรรม – ตัวชี้วัด (ยกเว้นแผนงานบุคคลากรภาครัฐ)	งบประมาณ 2569	งบรายจ่าย	ลักษณะการดำเนินการ	ที่มา/ความต้องการโครงการ	สถานที่ดำเนินการ/สถานภาพปัจจุบัน (ณ วันจัดทำคำขอ)	ผลสัมฤทธิ์ที่คาดว่าจะได้รับจากการใช้จ่ายงบประมาณ
1. แผนงานยุทธศาสตร์ป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง	**298.0500**					
1.1 โครงการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐานสากล **<u>ตัวชี้วัด</u>** **เชิงปริมาณ** : หน่วยงานที่มีการยกระดับศักยภาพให้มีคุณภาพ ไม่น้อยกว่า 300 หน่วยงาน **เชิงคุณภาพ :** ร้อยละความเชื่อมั่นของหน่วยงานเป้าหมายที่มีการยกระดับศักยภาพให้มีคุณภาพ ไม่น้อยกว่าร้อยละ 70	**185.8466**	**งบอุดหนุน**	การดำเนินการจัดซื้อจัดจ้าง	มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐานเพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารซีศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ระดับความสำเร็จในการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน
1. กิจกรรมระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	15.3365					
2. กิจกรรมยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรฐาน Global Cybersecurity Index (GCI)	6.3198					
3. กิจกรรมส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานเป้าหมาย	12.0000					
4. กิจกรรมยกระดับศูนย์บริหารจัดการภัยคุกคามไซเบอร์(Cyber Threat Management and Response Center Initiative)	18.1125					
5. กิจกรรมการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thai CERT)	88.8000					
6. กิจกรรมการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ National Cyber security Operation Center (NSOC)	20.5379					
7. กิจกรรมการทบทวนนโยบายและแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์	3.7571					
8. กิจกรรมห้องปฏิบัติการสำหรับการทดสอบเจาะระบบ (Penetration Testing Lab)	20.9828					

แผนงาน – ผลผลิต/โครงการ – กิจกรรม – ตัวชี้วัด (ยกเว้นแผนงานบุคคลากรภาครัฐ)	งบประมาณ 2569	งบรายจ่าย	ลักษณะการดำเนินการ	ที่มา/ความต้องการโครงการ	สถานที่ดำเนินการ/สถานภาพปัจจุบัน (ณ วันจัดทำคำขอ)	ผลสัมฤทธิ์ที่คาดว่าจะได้รับจากการใช้จ่ายงบประมาณ
1.2 โครงการเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ **<u>ตัวชี้วัด</u>** **เชิงปริมาณ** : จำนวนหน่วยงานได้รับการเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 60 หน่วยงาน **เชิงปริมาณ :** จำนวนบุคลากรทั้งเจ้าหน้าที่สายงานไอทีโดยตรงและเจ้าหน้าที่ทั่วไป (IT and non-IT) ได้รับการเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 1,000 ราย 1. กิจกรรมจัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (Thailand's National Cyber Exercise) 2. กิจกรรมการจัดตั้งสถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ 3.กิจกรรมพัฒนาและฝึกอบรมหลักสูตรระดับประกาศนียบัตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชน 4. กิจกรรมการสร้างความตระหนักรู้และพัฒนาทักษะเกี่ยวกับภัยคุกคามทางด้านไซเบอร์ (Cyber Top Talent) และแนะแนวอาชีพทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 5. กิจกรรมการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber SecurityLab)	**94.5917** 9.5780 34.3510 6.5116 3.3756 40.7755	**งบอุดหนุน**	การดำเนินการจัดซื้อจัดจ้าง	เสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยบูรณาการบุคลากร องค์ความรู้และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารซีศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ระดับความสำเร็จการเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ โดยบูรณาการ บุคลากร องค์ความรู้และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ
1.3 ผลผลิต ส่งเสริมการบริหารงานด้านความมั่นคงปลอดภัยไซเบอร์ **<u>ตัวชี้วัด</u>** **เชิงปริมาณ :** สนับสนุนการบริหารงานด้านความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 2 ด้าน	**11.6632**	**งบอุดหนุน**	ดำเนินการเอง	เพื่อเป็นค่าใช้จ่ายในการบริหารจัดการและดำเนินการตามภารกิจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งขาติ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารซีศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ระดับความสำเร็จในการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

แผนงาน – ผลผลิต/โครงการ – กิจกรรม – ตัวชี้วัด (ยกเว้นแผนงานบุคคลากรภาครัฐ)	งบประมาณ 2569	งบรายจ่าย	ลักษณะการดำเนินการ	ที่มา/ความต้องการโครงการ	สถานที่ดำเนินการ/สถานภาพปัจจุบัน (ณ วันจัดทำคำขอ)	ผลสัมฤทธิ์ที่คาดว่าจะได้รับจากการใช้จ่ายงบประมาณ
1.4 โครงการส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้ **<u>ตัวชี้วัด</u>** **เชิงคุณภาพ :** ร้อยละความสำเร็จของบุคลากรที่พัฒนาขีดความสามารถนำไปสู่การส่งเสริมบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ ร้อยละ 80 1. กิจกรรมการเตรียมความพร้อมระบบสารสนเทศเพื่อเข้าสู่ยุคควอนตัม	**3.6800** 3.6800	**งบอุดหนุน**	การดำเนินการจัดซื้อจัดจ้าง	เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารซีศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ระดับความสำเร็จการส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้
1.5 โครงการบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ **<u>ตัวชี้วัด</u>** **เชิงปริมาณ :** หน่วยงานที่มีการบูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์ ไม่น้อยกว่า 35 หน่วยงาน **เชิงปริมาณ :** กิจกรรมที่มีการบูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์ทั้งภายในและต่างประเทศ ไม่น้อยกว่า 35 ครั้ง 1. กิจกรรมการบูรณาการความร่วมมือ ในการป้องกันการละเมิดข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์ 2. กิจกรรมเสริมสร้างเครือข่ายความร่วมมือและดำเนินการตามพันธกรณีระหว่างประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ	**2.2685** 1.2480 1.0205	**งบอุดหนุน**	การดำเนินการจัดซื้อจัดจ้าง	การบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วนทั้งภายในประเทศและระหว่างประเทศ	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารซีศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ระดับความสำเร็จการบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์

แผนงาน – ผลผลิต/โครงการ – กิจกรรม – ตัวชี้วัด (ยกเว้นแผนงานบุคคลากรภาครัฐ)	งบประมาณ 2569	งบรายจ่าย	ลักษณะการดำเนินการ	ที่มา/ความต้องการโครงการ	สถานที่ดำเนินการ/สถานภาพปัจจุบัน (ณ วันจัดทำคำขอ)	ผลสัมฤทธิ์ที่คาดว่าจะได้รับจากการใช้จ่ายงบประมาณ
2. แผนงานบูรณาการรัฐบาลดิจิทัล **2.1 โครงการพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์** **<u>ตัวชี้วัด</u>** **เชิงคุณภาพ :** ความก้าวหน้าในการพัฒนางานบริการภาครัฐผ่านแพลตฟอร์มบริการกลางครอบคลุม ไม่น้อยกว่าร้อยละ 80 **เชิงคุณภาพ :** ความสำเร็จของการพัฒนาแพลตฟอร์มหรือเครื่องมือดิจิทัลกลางภาครัฐที่พร้อมเปิดให้ใช้บริการได้ตามแผนที่กำหนด ร้อยละ 100 **เชิงคุณภาพ :** มีหน่วยงานใช้บริการเพิ่มขึ้น และพร้อมรองรับการให้บริการทุกกรมที่เกี่ยวข้องหรือหน่วยงานเทียบเท่า ร้อยละ 10 1. กิจกรรมบูรณาการการเชื่อมโยงข่าวกรองทางไซเบอร์เพื่อเพิ่มประสิทธิภาพความแม่นยำในการคาดการณ์เหตุการณ์ภัยคุกคาม 2. กิจกรรมพัฒนาระบบศูนย์กลางข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะด้วยการตรวจจับและป้องกันภัยคุกคามขั้นสูงและการลดความเสี่ยงแบบเชิงรุก 3. กิจกรรมสนับสนุนการจัดตั้ง Sectoral CERT ด้านบริการภาครัฐที่สำคัญ	**149.8546** 25.1885 44.4920 80.1741	**งบอุดหนุน**	การดำเนินการจัดซื้อจัดจ้าง	1. เพื่อประสานความร่วมมือ ช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมระหว่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ Sectoral CERT ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหน่วยงานภายใต้กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) หน่วยงานภายใต้กระทรวงพาณิชย์ และหน่วยงานภาครัฐอื่น ๆ 2. เพื่อสามารถวิเคราะห์และหาต้นตอของเหตุการณ์ที่เกิดขึ้นได้อย่างชาญฉลาดโดยใช้ Engine ของตัวระบบในการทำ Advanced Analytics ผสานกับข้อมูลภัยคุกคามจากระบบต่าง ๆ ที่ สกมช. มีอยู่ได้ อาทิเช่น ระบบที่รวบรวมข้อบ่งชี้ภัยคุกคาม หรือ Threat Intelligence เป็นต้น 3. เพื่อเพิ่มประสิทธิภาพในการวิเคราะห์ รวบรวม และจัดเก็บข้อมูล ภัยคุกคามไซเบอร์ของประเทศ โดยสามารถแลกเปลี่ยนข้อมูลภัยคุกคามได้ทั้งภายในและภายนอกประเทศได้ 4. เพื่อยกระดับการตรวจจับภัยคุกคามและการตอบสนองต่อภัยคุกคามด้วย Advanced Threat Defense ที่มีความสามารถของ AI ในการสร้างรูปแบบการหลอกลวงที่เสมือนจริงได้แบบอัตโนมัติ เพื่อให้การตรวจจับที่รวดเร็วและแม่นยำในการปกป้องข้อมูล	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารซีศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	ระดับความสำเร็จในการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

คำชี้แจง : ให้ กรม/หน่วยงาน ยกตัวอย่างโครงการ/กิจกรรม ที่เป็นรายการสำคัญ ๆ ประจำปีงบประมาณ พ.ศ. 2569 ดังนี้

1. ให้ยกตัวอย่างโครงการสำคัญ ๆ ที่เห็นควรนำเสนอ **จำนวน 10-15 โครงการ**
2. **โครงการดังกล่าวจะต้องเป็นโครงการที่มีความสำคัญต่อการพัฒนาประเทศ สนับสนุนส่งเสริมหรือพัฒนาความเป็นอยู่ของประชาชน การแก้ไขปัญหา ที่เกิดขึ้น การเตรียมการวางแผนเพื่อรองรับปัญหาที่อาจเกิดขึ้น การป้องกันบรรเทาสาธารณภัย หรือการบริหารจัดการภัยพิบัติต่าง ๆ (ภัยที่กระทบต่อทรัพยากรธรรมชาติ-ภัยทางเศรษฐกิจ-ภัยทางสังคม-ภัยความมั่นคง) เป็นต้น โดยเน้นความสอดคล้องตามกลุ่มภารกิจของกระทรวงนั้น ๆ เป็นหลัก ได้แก่ กระทรวงด้านความมั่นคง กระทรวงด้านเศรษฐกิจ และกระทรวงด้านสังคม หรือบูรณาการประสานการสนับสนุนกลุ่มภารกิจในมิติด้านอื่นตามขอบเขตหน้าที่และอำนาจที่เกี่ยวข้อง**
3. สำหรับหน่วยงานอื่นที่ไม่สังกัดกระทรวงให้ยกตัวอย่างโครงการตามภารกิจของหน่วยงาน
4. ให้เรียงลำดับโครงการจากวงเงินงบประมาณ**มากไปหาน้อย**

5. ผลการเบิกจ่ายและผลการดำเนินงานในปีงบประมาณ พ.ศ. 2567-2568

(แบบ สว.69-03 (กรม/หน่วยงาน))

ผลการเบิกจ่ายและผลการดำเนินงานในปีงบประมาณ พ.ศ. 2567-2568

.....

ชื่อหน่วยงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

1. ภาพรวมผลการเบิกจ่ายงบประมาณ ประจำปีงบประมาณ พ.ศ. 2568

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

ประเภทรายจ่าย	วงเงินตาม พ.ร.บ. (1)	วงเงินหลังโอนเปลี่ยนแปลง (2)	ผลการเบิกจ่าย		ผลการใช้จ่าย	
			จำนวน (3)	ร้อยละ (4) = (3)/(2)*100	จำนวน (5)	ร้อยละ (6) = (5)/(2)*100
รวม	486.1870	-	486.1870	100.00	486.1870	100.00
รายจ่ายประจำ	227.1695	-	227.1695	100.00	227.1695	100.00
รายจ่ายลงทุน	259.0175	-	259.0175	100.00	259.0175	100.00

หมายเหตุ : ให้ใช้ผลการเบิกจ่าย **ณ วันที่ 30 เมษายน 2568** และคำนวณร้อยละจากวงเงินงบประมาณหลังโอนเปลี่ยนแปลง

2. การกันเงินไว้เบิกเหลื่อมปี ปีงบประมาณ 2567

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

ผลผลิต/โครงการ กิจกรรม	งบประมาณปี 2567					คำชี้แจง
	เงินกันไว้เบิกเหลื่อมปี	เบิกจ่าย	ร้อยละ	คงเหลือ	ร้อยละ	
รวม						
1.						ระบุ : สาเหตุ-แนวทางการดำเนินการเบิกจ่าย
2.	-ไม่มี-					
3.						
4.						
5.						

3. ผลการดำเนินงานในปีงบประมาณ พ.ศ. 2567-2568 ปัญหาอุปสรรค และแนวทางแก้ไข

3.1 ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการในปีงบประมาณ พ.ศ. 2567-2568

หน่วย : ล้านบาท (ทศนิยม 4 ตำแหน่ง)

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
	ปีงบประมาณ พ.ศ. 2567			
1.	โครงการส่งเสริมการวิจัย การสร้างองค์ความรู้และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	6.9293	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	มีฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ และมีอุปกรณ์และเครื่องมือพร้อมสำหรับงานวิจัยความมั่นคงปลอดภัยไซเบอร์
2.	โครงการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์	8.0000		พัฒนาขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่นๆ ที่เกี่ยวข้อง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562 ส่งผลให้ประเทศไทยมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีความพร้อมในการประสานงาน ป้องกันและรับมือภัยคุกคามทางไซเบอร์ในทุกมิติ
3.	โครงการยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรฐาน Global Cyber Index (GCI)	8.8880		1. สกมช. ยกระดับการพัฒนาดัชนีความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index : GCI) และการส่งเสริมและสนับสนุนการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐต่าง ๆ ให้เป็นมาตรฐานสากล และการเพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 2. รายงานผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (Cyber Resilience Assessment) ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ถูกนำไปใช้ในการจัดทำแนวทางการยกระดับการเตรียมพร้อมและการปรับตัวในระดับประเทศ (National Cyber Resilience Framework)

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
4.	โครงการมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์	6.3000	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	ทบทวนแบบประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่จัดทำโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์
5.	โครงการ Help Desk	10.3116		สกมช. เพื่อรองรับการแจ้งปัญหา การให้ความช่วยเหลือ การเตือนภัยทางไซเบอร์ได้หลากหลายช่องทางเพื่อการแก้ไขปัญหาอย่างทันท่วงที ลดหรือหลีกเลี่ยงความเสียหายทางไซเบอร์ อันนำมาซึ่งความมั่นคงปลอดภัยทางไซเบอร์ให้ทั้งภาครัฐ เอกชน และประชาชน
6.	โครงการยกระดับการประสานงานในการตอบสนองและแลกเปลี่ยนข้อมลูภัยคุกคามทางไซเบอร์	7.2066		หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานภาครัฐและภาคเอกชน มีเครื่องมือและแหล่งข้อมูลบ่งชี้ลักษณะภัยคุกคามไซเบอร์ที่มีความน่าเชื่อถือ สามารถใช้งานได้ง่าย มีความยืดหยุ่น ปรับแต่งการจัดการและบริหารให้เข้ากับแต่ละหน่วยงานในได้ และที่สำคัญระบบที่พัฒนาขึ้นจะสามารถช่วยลดค่าใช้จ่ายด้านการลงทุนเกี่ยวกับข้อมูลบ่งชี้ภัยคุกคามไซเบอร์ให้กับหน่วยงานต่าง ๆ ที่เข้าร่วมโครงการได้เป็นอย่างมาก ทำให้หน่วยงานสามารถเตรียมตัวรับมือกับภัยคุกคามได้รวดเร็วและเป็นระบบ จำกัดวงความเสียหายที่จะเกิดขึ้นกับทั้งข้อมูลสำคัญ และความเสียหายเชิงเศรษฐกิจ
7.	โครงการยกระดับการเฝ้าระวัง ตอบสนองรับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์	151.0850		1. หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ และหน่วยงานภาครัฐที่มีความสำคัญของประเทศ ได้รับการตอบสนองต่อภัยคุกคามทางไซเบอร์และรับมือได้อย่างทันท่วงที เมื่อเกิดเหตุการณ์ที่กระทบ ต่อความมั่นคงปลอดภัยทางไซเบอร์กับระบบที่สำคัญของหน่วยงาน และหรือระบบที่ให้บริการแก่ประชาชน 2. ประเทศไทยมีเครื่องมือ และทีมปฏิบัติการในการรับมือภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ 3. ประเทศไทยมีศูนย์ปฏิบัติการร่วมทางไซเบอร์ ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อประสานงานกับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อการแก้ไขปัญหาอย่างทันท่วงที 4. ประเทศไทยมีชุดเครื่องมือเผชิญเหตุภัยคุกคามทางไซเบอร์แบบเคลื่อนที่เร็ว (Cyber Mobile Team) ที่พร้อมปฏิบัติภารกิจ

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
8.	โครงการจัดทำแผนปฏิบัติการเพื่อการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุกคามไซเบอร์	14.7232	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	1. หน่วยงานเป้าหมายได้รับรายงานผลการประเมินความเสี่ยงในภาพรวมของประเทศ และระดับกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อนำไปใช้ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการกำหนดมาตรการเพื่อลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น ส่งผลให้ประเทศไทยมี Ecosystem ที่เอื้อต่อการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อการพึ่งพาตนเองในอนาคตอย่างยั่งยืน 2. สามารถจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Incident Response Plan) เพื่อรับมือกับเหตุภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ส่งผลให้ประเทศไทยมี Ecosystem ที่เอื้อต่อการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อการพึ่งพาตนเองในอนาคตอย่างยั่งยืน
9.	โครงการย้ายสำนักงาน ไป ณ ศูนย์ราชการ Zone C	61.7830		1. มีหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมและมีบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาขีดความสามารถผู้ปฏิบัติงานตามมาตรฐานสากล 2. ได้พัฒนาศักยภาพและเพิ่มทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับ เยาวชน นักเรียน และนักศึกษา 3. นักเรียน นักศึกษา หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หน่วยงานภาครัฐ ภาคเอกชน และประชาชนทั่วไป ได้รับการพัฒนาทักษะการเรียนรู้และประสบการณ์ด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ ตระหนักถึงภัยคุกคามด้านไซเบอร์ที่จะเกิดขึ้น และเป็นการกระตุ้นให้เกิดการแข่งขันในตลาดแรงงาน
10.	โครงการพัฒนาศักยภาพบุคลากรด้านไซเบอร์ ในทุกช่วงวัยและกลุ่มประชากร	13.9744		1. มีหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมและมีบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาขีดความสามารถผู้ปฏิบัติงานตามมาตรฐานสากล 2. ได้พัฒนาศักยภาพและเพิ่มทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับ เยาวชน นักเรียน และนักศึกษา 3. นักเรียน นักศึกษา หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หน่วยงานภาครัฐ ภาคเอกชน และประชาชนทั่วไป ได้รับการพัฒนาทักษะการเรียนรู้และประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตระหนักถึงภัยคุกคามด้านไซเบอร์ที่จะเกิดขึ้น และเป็นการกระตุ้นให้เกิดการแข่งขันในตลาดแรงงาน

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
11.	โครงการขับเคลื่อนนโยบายและแผนการรักษาความมั่นปลอดภัยไซเบอร์	3.4400	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	มีผลการติดตามและประเมินผลของหน่วยงานทุกภาคส่วนที่เกี่ยวข้อง อาทิ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานภาครัฐ หน่วยงานภาคเอกชน เพื่อสอดรับการขับเคลื่อนนโยบายและแผนฯ ไปสู่การปฏิบัติได้อย่างเป็นรูปธรรม และเกิดประสิทธิภาพประสิทธิผลสูงสุดในการรักษาความมั่นคงปลอดภัยไซเบอร์
12.	โครงการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Lead Implementer Lead Auditor)	7.4506		หลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ได้รับการปรับปรุงให้มีความทันสมัย และบุคลากรของหน่วยงานควบคุมและกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้รับการพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดดภัยไซเบอร์ พ.ศ. 2562
13.	โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์	19.6757		หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้อง สามารถแลกเปลี่ยนข้อมูลเชิงเทคนิคระหว่างกันเพื่อให้เกิดการป้องกัน และ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ อย่างมีประสิทธิภาพ และโต้ตอบต่อภัยคุกคามรูปแบบใหม่ ๆ ที่มีวิวัฒนาการเพิ่มขึ้นอย่างรวดเร็วได้ อย่างเป็นระบบและต่อเนื่องเพื่อรองรับสถานการณ์ความมั่นคงปลอดภัยไซเบอร์ทั้งในปัจจุบันและในอนาคต
14.	โครการสนับสนุนการจัดตั้ง Sectoral CERT	70.9390		มีเครื่องมือที่มีประสิทธิภาพ บุคลากรที่มีความพร้อม และองค์ความรู้เพื่อใช้ในการดำเนินงานในการรับมือ ป้องกัน ตรวจจับและโต้ตอบต่อภัยคุกคาม เพื่อลดการสูญเสียทางตัวเงิน และภาพลักษณ์ของความน่าเชื่อถือ ที่จะเกิดขึ้นจากการโจมตีของภัยคุกคามขั้นสูง เช่น มัลแวร์เรียกค่าไถ่ หรือรูปแบบการโจมตีอื่น ๆ เป็นการป้องกันไว้ก่อนที่จะเกิดการสูญเสียที่เกินกว่าเหตุ
15.	โครงการพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์	28.8309		สำนักงานปลัดกระทรวงสาธารณสุข สามารถร่วมมือกับหน่วยงานที่เกี่ยวข้องจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านสาธารณสุข เพื่อสนับสนุนการทำงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานโครงสร้างพื้นฐานด้านสาธารณสุข มีระบบสารสนเทศที่เป็นแพลตฟอร์มกลางในการประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ระหว่างหน่วยงานร่วมกัน สามารถเฝ้าระวัง ป้องกัน และรับมือภัยคุกคามได้อย่างมีประสิทธิภาพ

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
	ปีงบประมาณ พ.ศ. 2568			
1.	โครงการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐานสากล	205.4769	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	1. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติสามารถรองรับการแจ้งปัญหาเชิงรุกในหลายช่องทาง การให้ความช่วยเหลือการเตือนภัยทางไซเบอร์ และแจ้งวิธีการป้องกันแก้ไขปัญหาอย่างทันท่วงทีทำให้ลดความเสียหายจากภัยคุกคามทางไซเบอร์ได้ อันนำมาซึ่งความมั่นคงปลอดภัยทางไซเบอร์ ให้ทั้งภาครัฐ เอกชน ประชาชน และทำให้ประเทศมีความมั่นคง มีความน่าเชื่อถือด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น 2. หน่วยงานเป้าหมายทราบถึงระดับขีดความสามารถทางไซเบอร์ เมื่อเทียบกับค่าเฉลี่ยของหน่วยงานในระดับเดียวกัน ส่งผลให้หน่วยงานเป้าหมายสามารถวางแผน และมีมาตรการ/แนวทาง ในการยกระดับขีดความสามารถทางไซเบอร์ได้มีประสิทธิภาพมากยิ่งขึ้น 3. สกมช. ได้กรอบแนวทางในการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ในระยะยาวและส่งเสริมสนับสนุนการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐต่าง ๆ ให้เป็นมาตรฐานสากล และการเพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม รวมทั้งส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรที่ให้บริการที่สำคัญให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล มีแนวทางเพื่อให้ประเทศได้รับการจัดอันดับจากดัชนีการชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ในหมู่ประเทศสมาชิก ITU (GCI) ที่ดียิ่งขึ้น และสุดท้ายความสามารถในการแข่งขันและความเชื่อมั่นทางเศรษฐกิจของประเทศสูงขึ้น 4. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล (Regulator) และหน่วยงานภาครัฐที่มีความสำคัญของประเทศได้รับการช่วยเหลือในการตอบสนองต่อภัยคุกคามทางไซเบอร์และรับมือได้อย่างทันท่วงที เมื่อเกิดเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์กับระบบที่สำคัญของหน่วยงาน และหรือระบบที่ให้บริการแก่ประชาชน

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
				5. ประเทศไทยมีศูนย์ปฏิบัติการร่วมทางไซเบอร์ ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อประสานงานกับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 6. ประเทศไทยมีชุดเครื่องมือเผชิญเหตุภัยคุกคามทางไซเบอร์แบบเคลื่อนที่เร็ว (Cyber Mobile Team) ที่พร้อมปฏิบัติภารกิจ 7. หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงหน่วยงานอื่น ๆ ที่เกี่ยวข้อง ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สามารถยกระดับและเพิ่มขีดความสามารถในการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ 8. สกมช. จัดหาและพัฒนาระบบสารบรรณอิเล็กทรอนิกส์ E-Document พร้อมลายเซ็นอิเล็กทรอนิกส์ที่สามารถใช้งานต่อเนื่องให้สามารถ สนับสนุนงานหลักได้ทุกกระบวนงาน 1 ระบบ และพัฒนาระบบงบประมาณ การเงินและบัญชี และงานพัสดุ สำหรับสนับสนุนนงานการดำเนินงานของสำนักการเงินและกลยุทธ์องค์กรให้มีความครอบคลุมการสอดคล้องกับการปฏิบัติงาน จำนวน 1 ระบบ 9. สำนักงานมีแบบสถาปัตยกรรมภายในอาคารพื้นที่ ถูกต้องตามโครงสร้างหน่วยงาน และความต้องการในการปฏิบัติงาน 10. สำนักงานมีแแบบสถาปัตยกรรมในอาคาร สำหรับการใช้เป็นข้อมูลประกอบการขอรับการจัดสรรงบประมาณในการจ้างผู้รับจ้างที่มีฝีมือในการจัดทำและตกแต่งสำนักงาน 11. สำนักงานมีพื้นที่ที่เหมาะสมกับการปฏิบัติงาน และวัสดุ ครุภัณฑ์ที่จำเป็นเพียงพอต่อการปฏิบัติงานมีความทันสมัย สะดวก สะอาด ปลอดภัย รวมทั้งมีสภาพแวดล้อมที่เอื้ออำนวยต่อการปฏิบัติงาน 12. สำนักงานมีพื้นที่ปฏิบัติงานที่เหมาะสมสามารถขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยอย่างมีประสิทธิภาพ พร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์ในทุกมิติ 13. หน่วยงานเชื่อมต่อได้รับข้อมูลและแลกเปลี่ยนข้อมูลได้เพื่อทำการ Proactive Protection และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. เป็นแหล่งข้อมูลและศูนย์กลางของข่าว

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
				กรองของประเทศ ทำให้การป้องกันภัยคุกคามทางไซเบอร์ของประเทศมีประสิทธิภาพเพิ่มสูงขึ้น ส่งผลให้ความมั่นคงปลอดภัยไซเบอร์ของประเทศมีความมั่นคงและมีความน่าเชื่อถือเพิ่มมากขึ้น 14. บุคลากรของ สกมช. ได้รับการยกระดับสมรรถนะด้านความรู้ความสามารถด้านไซเบอร์ในระดับเป็นที่ยอมรับตามมาตรฐานสากลเพิ่มมากขึ้น ส่งผลให้ประเทศไทยได้รับการยอมรับในความมั่นคงปลอดภัยทางไซเบอร์และสามารถเป็นผู้นำสามารถรับมือความท้าทายด้านความปลอดภัยไซเบอร์ในทุกรูปแบบ นำไปสู่การมีบทบาทด้านองค์ความรู้ การถ่ายทอดความสามารถพร้อมรับมือภัยทางไซเบอร์ในทุกรูปแบบในทุกมิติเป็นที่ยอมรับในระดับสากลมากขึ้น ทั้งนี้ หากได้รับการสนับสนุนงบประมาณจะทำให้บุคลากรของ สกมช. เป็นผู้มีส่วนสำคัญของประเทศไทยให้สามารถกำหนดการมีส่วนร่วม และสร้างความเชื่อถือ ประสานความร่วมมือกับประเทศต่าง ๆ ในด้านการให้ความสำคัญด้านไซเบอร์ในระดับสากล 15. ประเทศชาติมีกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สามารถนำมาบังคับใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ทันสมัยสอดคล้องกับสภาวะการณ์เปลี่ยนแปลงของเทคโนโลยีในปัจจุบัน และไม่ก่อให้เกิดภาระแก่ประชาชนและหน่วยงานที่เกี่ยวข้องเกินความจำเป็น

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
2.	โครงการเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	115.2831	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	1. ประเทศไทยมีเครื่องมือ และทีมปฏิบัติการในการรับมือภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ 2. หลักสูตรผู้นำการปฏิบัติ (Lead Implementer) และหลักสูตรผู้นำการตรวจสอบ (Lead Auditor) ได้รับการปรับปรุงให้มีความทันสมัย และบุคลากรของหน่วยงานควบคุมและกำกับดูแล หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ได้รับการพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดดภัยไซเบอร์ พ.ศ. 2562 3. หน่วยงานเป้าหมาย สามารถยกระดับและเพิ่มขีดความสามารถในการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ 4. บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งในส่วนกลางและส่วนภูมิภาค ได้รับการพัฒนาทักษะและขีดความสามารถในการปฏิบัติงานตามมาตรฐานสากล สามารถนำความรู้ที่ได้ไปประยุกต์ใช้กับสถานการณ์ภัยคุกคามทางไซเบอร์ และมาตรการป้องกัน รับมือ จากภัยคุกคามทางไซเบอร์ พร้อมทั้งนำความรู้ที่ได้ไปถ่ายทอดต่อและปรับใช้ในการทำงานและเผยแพร่ต่อบุคคลอื่นได้ 5. นักเรียน นักศึกษา หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) หน่วยงานภาครัฐ ภาคเอกชนและประชาชนทั่วไป ได้รับการพัฒนาทักษะการเรียนรู้และประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตระหนักถึงภัยคุกคามด้านไซเบอร์ที่จะเกิดขึ้น และเป็นการกระตุ้นให้เกิดการแข่งขันในตลาดแรงงาน

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
3.	โครงการส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้	7.0106	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	1. ประเทศมีระบบการติดตามประเมินผลการดำเนินงานภายใต้นโยบายและแผนปฏิบัติการว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ พร้อมทั้งฐานข้อมูลที่ครบถ้วนสมบูรณ์ ทำให้สามารถนำไปใช้เพื่อต่อยอดในดำเนินการจัดทำแผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างครอบคลุม และเกิดประโยชน์สูงสุดต่อหน่วยงานด้านความปลอดภัยไซเบอร์ของประเทศ ที่จะส่งผลให้การจัดทำนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศที่สามารถตอบสนองต่อการป้องกัน รับมือภัยคุกคามทางไซเบอร์ ที่ส่งผลกระทบต่อการดำเนินชีวิตของประชาชนมีประสิทธิภาพสูงสุด 3. หน่วยงานเป้าหมายได้รับรายงานผลการประเมินความเสี่ยงในภาพรวมของประเทศและระดับกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพื่อนำไปใช้ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์รวมถึงการกำหนดมาตรการเพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น 4. เพิ่มศักยภาพโครงสร้างพื้นฐาน ฐานข้อมูลการวิจัยและนักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพและขอบเขตการทำงานสูงขึ้น ก่อให้เกิดการเชื่อมโยงเครือข่ายงานวิจัยและนักวิจัยทั้งภายในและภายนอกประเทศ ส่งเสริมความร่วมมือการพัฒนางานวิจัยและเทคโนโลยีผ่านฐานข้อมูลเครือข่ายนักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ส่งผลให้เกิดการแข่งขันทั้งในด้านวิชาการ เทคโนโลยี และการคิดค้นผลิตภัณฑ์/บริการให้เพิ่มขึ้นทั้งในเชิงคุณภาพและปริมาณ สร้างความแข็งแกร่งของประเทศด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศผ่านการพัฒนาผลิตภัณฑ์/บริการจากการต่อยอดงานวิจัยที่เพิ่มขึ้น

ลำดับ	ชื่อ โครงการ-กิจกรรม	งบประมาณ	พื้นที่ดำเนินการ	ผลสำเร็จและประโยชน์ที่ได้รับจากการดำเนินโครงการ
4.	โครงการพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์	77.5601	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เลขที่ 120 หมู่ 3 ชั้น 7 อาคารรัฐศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานในแต่ละด้าน หน่วยงานรัฐ หน่วยงานควบคุมและกำกับดูแล มีระบบแพลตฟอร์มกลางเพื่อสนับสนุนการจัดตั้ง Sectoral CERT แบบรวมศูนย์ (Centralized Sectoral CERT Management Platform Development) เพื่อใช้ในการเฝ้าระวัง ตรวจจับและโต้ตอบภัยคุกคาม โดยระบบที่ดำเนินการนี้จะสามารถทำให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานในแต่ละด้าน หน่วยงานรัฐ หน่วยงานควบคุมและกำกับดูแล เห็นภาพรวมของเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยง รวมถึงเหตุการณ์การที่มีการโจมตีของระบบ Sectoral CERT ของหน่วยงานต่าง ๆ ได้ และสามารถส่งไปยังระบบ MISP ที่มีอยู่เดิมของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ เพื่อให้หน่วยงานต่าง ๆ ดำเนินการป้องกันและรับมือได้อย่างทันท่วงที ซึ่งทำให้ระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีประสิทธิภาพเพิ่มสูงขึ้น ทำให้ประเทศมีความน่าเชื่อถือและมีความมั่นคงปลอดภัยทางไซเบอร์สูงขึ้น

คำชี้แจง : ให้หน่วยรับงบประมาณ**ยกตัวอย่างการดำเนินโครงการที่ดำเนินการในปีงบประมาณ พ.ศ. 2567-2568** และเห็นว่าเป็นโครงการสำคัญที่ควรนำเสนอ

3.2 ปัญหา อุปสรรค และแนวทางแก้ไข (ข้อมูลปีงบประมาณ 2567-2568)

ลำดับ	ปัญหา-อุปสรรค	แนวทางแก้ไข
	1) ด้านการใช้จ่ายงบประมาณ - ไม่มี - 2) ด้านการดำเนินงาน	- ไม่มี -

6. การดำเนินการตามข้อสังเกตของคณะกรรมาธิการวิสามัญพิจารณาศึกษาร่างพระราชบัญญัติงบประมาณ รายจ่ายประจำปีงบประมาณ พ.ศ. 2568 วุฒิสภา

(แบบ สว.69-04 (กรม/หน่วยงาน))

สว.69-04 (กรม/หน่วยงาน)

การดำเนินการตามข้อสังเกตของคณะกรรมาธิการวิสามัญพิจารณาศึกษา
ร่างพระราชบัญญัติงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2568 วุฒิสภา

.....

ชื่อหน่วยงาน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประเด็นข้อสังเกต	การดำเนินการ
1. มีภารกิจสำคัญในการสกัดกั้นการกระทำความผิดที่เกิดจากภัยด้านไซเบอร์แต่หากพิจารณาจำนวนบุคลากรและงบประมาณที่ได้รับค่อนข้างน้อย จึงควรเพิ่มจำนวนบุคลากรให้เพียงพอโดยการจัดสรรงบประมาณให้เหมาะสม รวมถึงการกำหนดแนวทางในการดึงดูดให้บุคลากรที่มีศักยภาพสูงเข้ามาร่วมดำเนินงาน ตลอดจนควรมีการสร้างเครือข่ายเพื่อระดมบุคลากรที่เกี่ยวข้องจากหน่วยงานต่าง ๆ มาดำเนินการร่วมกันให้การปฏิบัติภารกิจเป็นไปอย่างมีประสิทธิภาพ	**1. มีภารกิจสำคัญในการสกัดกั้นการกระทำความผิดที่เกิดขึ้นจากภัยด้านไซเบอร์แต่หากพิจารณาจำนวนบุคลากรและงบประมาณที่ได้รับค่อนข้างน้อยจึงควรเพิ่มจำนวนบุคลากรให้เพียงพอโดยการจัดสรรงบประมาณให้เหมาะสมรวมถึงการกำหนดแนวทางในการดึงดูดให้บุคลากรที่มีศักยภาพสูงเข้ามาร่วมดำเนินงานตลอดจนควรมีการสร้างเครือข่ายเพื่อระดมบุคลากรที่เกี่ยวข้องจากหน่วยงานต่าง ๆ มาดำเนินการร่วมกัน ให้การปฏิบัติภารกิจเป็นไปอย่างมีประสิทธิภาพ** ด้วยสถานการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบันเกิดขึ้นอย่างรวดเร็วและส่งผลกระทบเป็นวงกว้างต่อโครงสร้างพื้นฐานสำคัญของประเทศ หน่วยงาน องค์กร จนไปถึงระดับประชาชนที่ได้รับผลกระทบจากอาชญากรรมไซเบอร์ทั้งจากภายในประเทศและต่างประเทศ ประเทศไทยจึงได้ประกาศใช้ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นองค์การมหาชนที่จัดตั้งขึ้นตามมาตรา ๒๒ และเป็นหน่วยงานหลักที่สร้างกลไกในการขับเคลื่อนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอย่างยิ่งหน่วยงานของรัฐที่เป็นหน่วยงานในลักษณะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ทั้ง ๗ ด้าน ได้แก่ ด้านความมั่นคงภาครัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงิน การธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค และด้านสาธารณสุข หากพบข้อบกพร่องของการรักษาความมั่นคงปลอดภัยของระบบหรือข้อมูลของหน่วยงานต่าง ๆ ให้เร่งประสานแจ้งเตือนช่องโหว่หรือการรั่วไหลของข้อมูลส่วนบุคคลแก่หน่วยงานนั้นเพื่อระงับยับยั้งไม่ให้เกิดความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นโดยเร็ว รวมทั้งการกำหนดนโยบาย กำหนดกรอบมาตรฐานและแนวทางการปฏิบัติ และการอบรมให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงมากขึ้นในปัจจุบัน **2. สกมช. มีการดำเนินการที่ผ่านมาโดยได้ดำเนินการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมทั้งปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศสรุปผลการปฏิบัติตั้งแต่ปี พ.ศ. 2564 ถึงปัจจุบัน ได้ดังนี้**

ประเด็นข้อสังเกต	การดำเนินการ
	(1) มีหนังสือแจ้งเตือนหน่วยงานเกี่ยวกับช่องโหว่เพื่อป้องกันก่อนเกิดเหตุ (2) การเฝ้าระวัง แจ้งเตือนและแก้ไขเพื่อป้องกันหน่วยงานทั้งรัฐและเอกชนก่อนมีการรั่วไหล (3) การเฝ้าระวังติดตามและตรวจสอบกรณีข้อมูลรั่วไหลหน่วยงานทั้งรัฐและเอกชน (4) การจัดทำรายงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในแต่ละด้านให้กับหน่วยงานเพื่อติดตาม เฝ้าระวัง ตรวจสอบวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ประกอบด้วย รายงานการปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ ผลสรุปการสืบสวนวิเคราะห์ (Investigation) และการตรวจจับภัยคุกคามเชิงรุก (Threat Hunting) ผลสรุปการสืบสวนตรวจพิสูจน์หลักฐาน (Digital Forensic) และการทำวิศวกรรมย้อนกลับ (reverse engineering) ผลสรุปการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ เพื่อทดสอบความปลอดภัย (Penetration Testing) และผลการดำเนินงานที่สำคัญอื่น ๆ (5) สถานการณ์ภัยคุกคามทางไซเบอร์ ในปี พ.ศ. 2565 ที่ผ่านมามีสถิติภัยคุกคามที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข คิดเป็นร้อยละ 12 จากโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง 7 ด้าน แต่ในปัจจุบัน สกมช. ได้สนับสนุนและส่งเสริมให้หน่วยงานด้านสาธารณสุขจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข (Health CERT) เพื่อทำหน้าที่ประสานงานเฝ้าระวัง รับมือและแก้ไขภัยคุกคามทางไซเบอร์ด้านสาธารณสุข อีกทั้ง สกมช. ยังได้ดำเนินการเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง รวมทั้ง สกมช. ได้ให้การสนับสนุนหน่วยงานด้านสาธารณสุขได้มีการตอบสนองและแก้ไข ซึ่งปัจจุบัน สกมช. อยู่ระหว่างสนับสนุนการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านอื่น ๆ **3. การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ** หน่วยงานภาครัฐและภาคเอกชนให้ความสำคัญกับการป้องกัน รับมือจากภัยคุกคามไซเบอร์ เพิ่มมากขึ้น ดังที่ได้พบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน CII) เพิ่มขึ้นจากปี 2565 จำนวน 35 หน่วยงาน เป็น 63 หน่วยงานในปี 2566 แต่หลายหน่วยงานยังขาดความเข้าใจในการปฏิบัติตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และมีองค์ความรู้ในการดำเนินการตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ไม่เพียงพอ รวมถึงการขับเคลื่อนนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยังไม่ครอบคลุมครบถ้วนตามที่กำหนด และยังมีหน่วยงานที่เกี่ยวข้องจำนวนหลายหน่วยงานยังไม่ดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ แต่อย่างใด ประกอบกับกำลังคนของ สกมช. ไม่เพียงพอในการสนับสนุนปัญหาดังกล่าวของหน่วยงานข้างต้นได้อย่างทั่วถึง

ประเด็นข้อสังเกต	การดำเนินการ
	อย่างไรก็ดี สกมช. ได้ปฏิบัติภารกิจการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเต็มความสามารถ โดยมีการรายงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ที่มีนายกรัฐมนตรีเป็นประธาน โดยตำแหน่งอย่างต่อเนื่อง รวมทั้งรายงานต่อคณะรัฐมนตรีสำหรับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญ แต่เนื่องด้วยเทคโนโลยีที่มีการเปลี่ยนแปลงและพัฒนาอย่างรวดเร็วจึงทำให้เกิดภัยคุกคามด้านไซเบอร์มีจำนวนมากและรุนแรงส่งผลกระทบต่อเศรษฐกิจและสังคมของประเทศในวงกว้าง 1.1 Manpower Planning ปัจจุบันสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีพนักงานที่ปฏิบัติงานจำนวน 120 คน โดยเป็นพนักงานที่ปฏิบัติภารกิจหลักจำนวน 45 คนและภารกิจทางงานสนับสนุนจำนวน 75 คน ทั้งนี้ หากเทียบตามกรอบอัตรากำลังที่มีอยู่ในปัจจุบันของ สกมช. คิดเป็นเพียงร้อยละ 25 ของกรอบอัตรากำลังเต็มจำนวน 480 อัตรา จากกรอบอัตรากำลังทั้งหมด (มติที่ประชุมคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ครั้งที่ 1/2563 เมื่อวันที่ 8 กันยายน 2563 เห็นชอบให้ สกมช. บรรจุพนักงาน 480 อัตรา ภายในเวลา 2 ปี ซึ่งต้องดำเนินการตามกรอบระเวลาเสร็จสิ้นในปี 2565 แต่ปัจจุบัน สกมช. ดำเนินการบรรจุบุคลากรเพียง 120 คน) ประกอบกับภารกิจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ต้องปฏิบัติภารกิจเพื่อเตรียมพร้อมการรับมือความปลอดภัยทางไซเบอร์ตลอด 24 ชั่วโมง ทำให้บุคลากรที่มีอยู่ไม่เพียงพอต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ จึงทำบุคลากรของ สกมช. ที่มีอยู่ไม่สามารถรองรับปริมาณภัยคุกคามที่เกิดขึ้นกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ และประชาชนได้ ทำให้ส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ ดังนั้น การป้องกันและสกัดกั้นการกระทำความผิดจากภัยด้านไซเบอร์เป็นภารกิจที่มีความสำคัญอย่างยิ่งในยุคปัจจุบันที่เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทในทุกภาคส่วนของชีวิตประจำวัน การกระทำผิดทางไซเบอร์มีผลกระทบทั้งในด้านเศรษฐกิจ ความมั่นคง และความเป็นส่วนตัวของประชาชน ดังนั้น การจัดการและตอบสนองต่อภัยคุกคามดังกล่าวจึงต้องใช้ความร่วมมือจากหลายหน่วยงาน ทั้งนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีภารกิจในการดูแลความมั่นคงด้านไซเบอร์ของประเทศ จำเป็นต้องมีการเพิ่มจำนวนบุคลากรและทรัพยากรที่เหมาะสมเพื่อตอบสนองภารกิจ ที่สำคัญนี้ได้อย่างมีประสิทธิภาพ ซึ่งปัจจุบันสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้รับงบประมาณและบุคลากรที่ค่อนข้างจำกัด ส่งผลต่อการปฏิบัติภารกิจให้มีประสิทธิภาพลดลง ดังนั้นการเพิ่มจำนวนบุคลากรที่มีความรู้และความสามารถในด้านความมั่นคงไซเบอร์จึงเป็นสิ่งจำเป็นโดยการจัดสรรงบประมาณให้เหมาะสมและตรงตามความต้องการจะช่วยเสริมความสามารถในการรับมือกับภัยคุกคามที่เกิดขึ้นในโลกไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็วการจัดสรรงบประมาณเพื่อเพิ่มบุคลากรที่มีความสามารถสูงจึงต้องพิจารณาทั้งในด้านการฝึกอบรมพัฒนาทักษะของบุคลากรที่มีอยู่

ประเด็นข้อสังเกต	การดำเนินการ
	และการดึงดูดผู้ที่มีความเชี่ยวชาญด้านความมั่นคงไซเบอร์เข้ามาร่วมงาน การตั้งกลยุทธ์ในการดึงดูดบุคลากรที่มีศักยภาพสูงเช่นการเสนอเงินเดือนที่แข่งขันได้ หรือการสร้างสวัสดิการที่ดี รวมถึงการให้โอกาสในการพัฒนาอาชีพที่ก้าวหน้า จะช่วยให้หน่วยงานสามารถดึงดูดและรักษาบุคลากรที่มีคุณภาพได้ 1.2 ด้านการแข่งขันทางการตลาดแรงงาน ปัจจุบันสายวิชาชีพทางด้าน cyber security เมื่อเทียบกับความต้องการของตลาดแรงงานมีความต้องการเป็นอย่างสูงทั้งในภาครัฐและเอกชน ปัจจุบันมีสถานศึกษาที่ผลิตบุคลากรทางด้านนี้มาเป็นจำนวนน้อย จากผลการสำรวจของ สกมช. มีมหาวิทยาลัยจำนวน 21 แห่ง ที่มีการเรียนการสอนเป็นรายวิชาด้านความมั่นคงปลอดภัยไซเบอร์แต่อยู่ในกลุ่มวิชาเลือกโดยอยู่ในสาขาวิชาด้านเทคโนโลยีสารสนเทศ วิทยาการคอมพิวเตอร์ และคอมพิวเตอร์ธุรกิจ โดยยังไม่มีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เป็นการเฉพาะทั้งในระดับ ปริญญาตรี ปริญญาโท และปริญญาเอก ทั้งนี้มหาวิทยาลัยที่ยังไม่มีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์ ส่วนใหญ่เนื่องจากขาดแคลนบุคลากร เป็นสาเหตุหลักและสำคัญ จึงทำให้บุคลากรไม่เพียงพอในตลาดแรงงานและจากการสำรวจค่าจ้างทางสายงาน cyber security พบว่ามีค่าเฉลี่ยอยู่ที่ 39,000 - 205,000 (อ้างอิงตามผลสำรวจของ Manpower Group Thailand) เมื่อเทียบกับอัตราเงินเดือนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีอัตราเงินเดือนเฉลี่ยอยู่ที่ 31,200 - 152,000 ทำให้บุคลากรในสายวิชาชีพดังกล่าวถูกดึงตัวและไปปฏิบัติงานในภาคเอกชนจำนวนมาก นอกจากนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้สร้างเครือข่ายและความร่วมมือระหว่างหน่วยงานต่าง ๆ ในระดับทั้งภาครัฐและเอกชนก็เป็นอีกหนึ่งกลยุทธ์ที่สำคัญในการเสริมสร้างความมั่นคงไซเบอร์ การร่วมมือกับหน่วยงานต่าง ๆ จะช่วยให้มีการแลกเปลี่ยนข้อมูลและประสบการณ์ในการรับมือกับภัยคุกคาม รวมถึงสามารถระดมบุคลากรจากหลายแหล่งมาร่วมมือในการรับมือกับสถานการณ์ต่าง ๆ ได้อย่างมีประสิทธิภาพ การร่วมมือกับหน่วยงานภายนอก เช่น การสร้างความสัมพันธ์กับมหาวิทยาลัยและสถาบันการศึกษาต่าง ๆ ก็เป็นการส่งเสริมการผลิตบุคลากรที่มีความเชี่ยวชาญในด้านนี้ โดยการร่วมกันพัฒนาหลักสูตรการศึกษาให้ตรงกับความต้องการด้านไซเบอร์ หรือการฝึกอบรมร่วมระหว่างหน่วยงานต่าง ๆ เพื่อให้เกิดการแลกเปลี่ยนความรู้และทักษะในการเฝ้าระวังและป้องกันภัยคุกคามทางไซเบอร์ 1.3 จากการวิเคราะอัตรากำลัง ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยใช้วิธีการหา FTE (Full-Time Equivalent) ของพนักงาน เมื่อเดือนธันวาคม 2567 โดยมีที่ปรึกษาภายนอกเป็นผู้ให้คำแนะนำ พบว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีภาระงานปัจจุบันที่ต้องใช้บุคลากรอีกจำนวน 165 คน แต่ปัจจุบันมีบุคลากรปฏิบัติงานจำนวนเพียง 120 คน ซึ่งปัจจุบันได้ใช้วิธีการรับลูกจ้างเพื่อมาช่วยปฏิบัติภารกิจดังกล่าว หากมองในเชิงการปฏิบัติภารกิจหลักของหน่วยงานอาจมีผลกระทบต่อการทำงานในระยะยาวได้ซึ่งพบว่า สกมช. มีภาระงานปัจจุบันที่ต้องใช้บุคลากรถึง 285

ประเด็นข้อสังเกต	การดำเนินการ
	คน แต่ปัจจุบันมีบุคลากรปฏิบัติงานเพียง 120 คน เท่านั้น ยังขาดบุคลากรอีก 165 อัตรา เพื่อมาปฏิบัติงานขับเคลื่อนภารกิจงานของ สกมช. จึงสรุปได้ว่า การเพิ่มจำนวนบุคลากรที่มีทักษะสูงในด้านไซเบอร์ การจัดสรรงบประมาณที่เหมาะสม และการสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนเป็นปัจจัยที่สำคัญในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ การบริหารจัดการทรัพยากรบุคลากรและงบประมาณอย่างมีประสิทธิภาพจะทำให้การปฏิบัติภารกิจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สามารถตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างรวดเร็วและมีประสิทธิภาพ ฉะนั้นเพื่อให้การดำเนินการตอบสนองต่อภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ และรองรับการสนับสนุนการดำเนินให้แก่หน่วยงานรัฐหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สกมช. จึงเร่งดำเนินการบรรจุและแต่งตั้งพนักงานที่มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เหมาะสม และครบตามแผนการบรรจุที่คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ได้อนุมัติไว้โดย สกมช. ได้รับอนุมัติอัตราพนักงาน (อัตราเต็ม) จำนวน 480 อัตรา กบส. ได้อนุมัติแผนการบรรจุไว้ 2 ระยะ ระยะแรก 240 อัตรา และระยะสอง 240 อัตรา ซึ่ง สกมช. มีแผนจะบรรจุพนักงานในปีงบประมาณ พ.ศ. 2567 ให้ได้ 120 อัตรา จึงมีความจำเป็นต้องเพิ่มกรอบอัตราจากเดิม 121 อัตรา ในปีงบประมาณ 2569 ขอรับจัดสรรเพิ่มอีก 120 อัตรา รวมทั้งสิ้น 241 อัตรา โดยมีอัตราส่วนร้อยละ 70 : 30 คือ พนักงานกลุ่มวิชาชีพเฉพาะด้านไซเบอร์คิดเป็นร้อยละ 70 พนักงานกลุ่มปฏิบัติงานทั่วไป คิดเป็นร้อยละ 30 จากสัดส่วนของอัตรากำลังเน้นไปภารกิจในด้านการป้องกัน เฝ้าระวังภัยคุกคามเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ทั้งในภาครัฐและเอกชน หากเกิดภัยคุกคามและป้องกันไม่ได้ทันท่วงทีอาจเกิดความเสียหายที่มิอาจประเมินมูลค่าได้ที่มีผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ และส่งผลต่อความเชื่อมั่นต่อการลงทุนด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางด้านดิจิทัล โดยมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ National Computer Emergency Response Team (NCERT) : ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และศูนย์แจ้งเหตุภัยคุกคามทางไซเบอร์ รวมทั้งการประสานความร่วมมือทั้งในและต่างประเทศในการขับเคลื่อนการปกป้อง เฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ จึงมีความจำเป็นในการขอรับจัดสรร งบประมาณในแผนงานบุคลากรภาครัฐ จำนวน 161,286,300 บาท (หนึ่งร้อยหกสิบเอ็ดล้านสองแสนแปดหมื่นหกพันสามร้อยบาทถ้วน) รวมขอรับจัดสรรกรอบอัตรากำลังเพิ่มอีก 120 อัตราให้ครบจำนวน 240 อัตรา รวมทั้งค่าใช้จ่ายด้านบุคลากรที่เป็นขวัญและกำลังใจแก่พนักงานของ สกมช. ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ประเด็นข้อสังเกต	การดำเนินการ
2. ควรเพิ่มการประชาสัมพันธ์เผยแพร่ให้ประชาชนได้รับทราบช่องทางการติดต่อสื่อสารหรือขอความช่วยเหลือมากยิ่งขึ้น กรณีหากได้รับความเสียหายจากการถูกหลอกลวงที่มาจากภัยไซเบอร์	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีชื่อย่อว่า “สกมช.” เป็นหน่วยงานของรัฐในรูปแบบองค์การมหาชน ซึ่งมุ่งเน้นการบริหารและดำเนินงานอย่างมีประสิทธิภาพ เพื่อเป็นหน่วยงานกลาง สร้างกลไกขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามทางไซเบอร์ รวมทั้งให้ความช่วยเหลือ สนับสนุน ให้ความรู้ ความเข้าใจให้หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และประชาชน เพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่อาจเกิดขึ้น ที่ผ่านมาการประชาสัมพันธ์หรือการสร้างการรับรู้ภารกิจ บทบาท ตลอดจนการสร้างความเชื่อมั่นในการเป็นหน่วยงานที่ดูแลความมั่นคงปลอดภัยทางไซเบอร์ของประเทศเป็นไปอย่างมีข้อจำกัด เนื่องจากไม่ได้รับการจัดสรรงบประมาณ อาจมีบ้างก็เป็นเพียงงบดำเนินงานเพียงเล็กน้อย ซึ่ง สกมช. ก็ได้เพิ่มการประชาสัมพันธ์ เพื่อให้ประชาชนรับทราบช่องทางการติดต่อสื่อสารหรือขอความช่วยเหลือในกรณีที่ได้รับความเสียหายจากภัยไซเบอร์ เช่น การถูกหลอกลวงหรือโจมตีทางออนไลน์ ดังนี้ 1. สร้างแคมเปญประชาสัมพันธ์เชิงรุก โดยใช้โซเชียลมีเดียและสื่อต่าง ๆ เช่น YouTube, Facebook, และ TikTok ในการให้ข้อมูลเกี่ยวกับการเตือนภัย วิธีการป้องกันภัยไซเบอร์ และแนะนำช่องทางช่วยเหลือ รวมถึงการนำเสนอข่าวสารรวมกว่า 645 ครั้ง 2. เพิ่มช่องทางการติดต่อที่เข้าถึงง่าย ได้แก่ รับแจ้งเหตุภัยคุกคามทางไซเบอร์ 02-1143531 (24 ชั่วโมง) และเปิดให้แจ้งเหตุผ่านแอปพลิเคชันหรือแพลตฟอร์มออนไลน์ที่ THCert Helpdesk 3. จัดอบรมและกิจกรรมเพื่อสร้างความตระหนักรู้ 3.1 โครงการรู้เท่า รู้ทัน รู้ป้องกันภัยไซเบอร์ โดยดำเนินการจัดกิจกรรมอบรมในพื้นที่ 4 ภูมิภาค จำนวน 8 จังหวัด ประเทศไทย เพื่อให้ความรู้และสร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยไซเบอร์และด้านการคุ้มครองข้อมูลส่วนบุคคลให้กับประชาชนทุกช่วงวัยทั่วประเทศ รวมถึงส่งเสริมความรู้ความเข้าใจในการใช้งานอินเทอร์เน็ตให้ปลอดภัย 3.2 NCSA Cybersecurity Knowledge Sharing จำนวน 10 ครั้ง เพื่อเป็นการเสริมความรู้ให้กับบุคลากรผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ ให้มีความรู้ความเข้าใจ เพื่อสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ ให้ทราบถึงข้อมูลรายงานทิศทางของภัยคุกคาม ในระดับประเทศและระดับโลก ให้กับผู้เข้าร่วมรับฟังเพื่อเตรียมรับมือให้เท่าทันภัยคุกคามทางไซเบอร์อยู่ตลอดเวลา 3.3 กิจกรรมค่ายเยาวชนไซเบอร์ (Cyber Youth Camp) มุ่งเน้นพัฒนาทักษะด้านไซเบอร์และเทคโนโลยีสารสนเทศให้กับเยาวชน รุ่นที่ 1 วันที่ 15-17 ตุลาคม 2567 ณ ศูนย์ฝึกอบรมบริบาลบ้านผู้หว่าน จังหวัดนครปฐม และรุ่นที่ 2 วันที่ 25-27 ตุลาคม 2567 ณ สวนสัตว์เปิดเขาเขียว จังหวัดชลบุรี 3.4 กิจกรรมจัดการแข่งขันทักษะทางไซเบอร์ (Cyber Top Talent) เพื่อยกระดับความสามารถของบุคลากรไทย (ระดับมัธยมศึกษา อุดมศึกษา และประชาชนทั่วไป)

ประเด็นข้อสังเกต	การดำเนินการ
	4. สื่อประชาสัมพันธ์ในรูปแบบที่หลากหลาย จัดทำ Infographic, วิดีโอสั้น หรือแอนิเมชัน ที่เข้าใจง่าย และสื่อถึงอันตรายจากภัยไซเบอร์ จำนวน 50 ชิ้นงาน 5. สร้างเครือข่ายความร่วมมือกับชุมชนและองค์กรท้องถิ่น รวมถึงภาคีเครือข่ายกว่า 10 หน่วยงาน ในการประชาสัมพันธ์ข้อมูลไปยังชุมชนองค์กรปกครองส่วนท้องถิ่น หรือสถานศึกษา เพื่อช่วยเผยแพร่ข้อมูลไปถึงประชาชนในวงกว้าง จำนวน 15 ชิ้นงาน 6. ขยายช่องทางประชาสัมพันธ์ผ่านรายการวิทยุ ใช้รายการวิทยุในระดับท้องถิ่นและระดับประเทศในการให้ข้อมูล เช่น การให้คำแนะนำในการป้องกันภัยไซเบอร์ ผ่านรายการวิทยุจำนวน 2 รายการ ได้แก่ รายการสายลับไซเบอร์ F.M. 96.0 MHz จำนวน 19 ตอน และรายการภัยร้ายจากไซเบอร์ วิทยุ อสมท. FM 95 Mhz จังหวัดศรีสะเกษ และวิทยุ อสมท FM 107.0 MHz. จังหวัดอุบลราชธานี ซึ่งจะเห็นได้ว่า แม้ สกมช. จะพยายามประชาสัมพันธ์ ผ่านช่องทางต่าง ๆ ดังกล่าว โดยไม่ใช้งบประมาณ แต่ด้วยเนื้อหา และช่องทางการเผยแพร่ยังไม่น่าสนใจและครอบคลุม หากได้รับการจัดสรรงบประมาณในการประชาสัมพันธ์ก็จะสร้างการรับรู้และความเชื่อมั่นให้กับประชาชนและลดความสูญเสียทรัพย์สินของประชาชนได้มากกว่านี้