



รูปภาพเครื่องสำรองไฟ UPS Riello ขนาด ๑๐ KVA จำนวน ๒ เครื่อง

๑๓. ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ของกรมฯ (dmcr.mail.go.th)

๑๓.๑ บัญชีผู้ใช้งานรวมทั้งหมด ๘๓๘ บัญชี

๑๓.๒ พื้นที่การใช้งานรวม ๕๐ GB

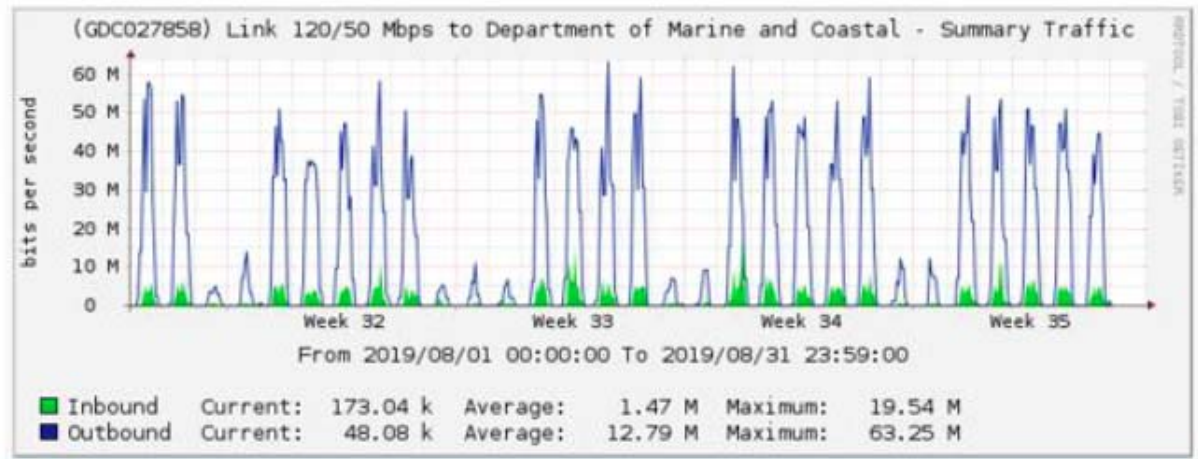
๑๓.๓ รายชื่อบัญชีผู้ใช้งานที่มีเนื้อที่ใช้งานสูงสุดจำนวน ๒๐ บัญชี

1	ชื่อ-นามสกุล	เนื้อที่ ที่ใช้ไป (MB)	สถานะ
2	สลก อาทิตา จุ้ยเอี่ยม	8098.27	active
3	กคณ จิราภรณ์ วัชรสินธุ์	5653.72	locked
4	สปลล ปาณิสรา ภัทรกมลภรณ์	4308.87	locked
5	ศูนย์วิจัยและพัฒนาทรัพยากรทางทะเลและ	1860.42	locked
6	สวพ นิพนธ์ พงศ์สุวรรณ	1677.83	locked
7	สปลล ชاکรี รอดไฟ	1410.22	locked
8	กผง ฝ่ายแผนงาน กผง	1227.7	active
9	สปลล ปทีตดา โกสุวรรณ	1138.88	active
10	ศสท ศูนย์สารสนเทศ กผง	1002.9	active
11	กพร พัชรพร เขาเห็น	978.09	locked
12	กพร นิตญา ลุนสมบัติ	954.62	active
13	สวพ ศูนย์วิจัยดองกลาง สงขลา	883.06	active
14	สปลล วิทยา ศิริแสง	840.27	active
15	สทช นิพนธ์ ทองอู๋	784.85	locked
16	ศสท ณัฐพล บุญยีน	672.64	active
17	สปลล ปรียา ชมเขย	654.71	active
18	สทช สมหญิง พวงประสาน	634.03	active
19	ศสท ณัฐสิทธิ์ เขื่อนคำจันทร์	591.5	active
20	สปลล บุญญาพร ทองแท่น	579.95	locked
21	Webmaster กรมทรัพยากรทางทะเลและ	547.85	locked

หมายเหตุ : สำนักงานรัฐบาลอิเล็กทรอนิกส์(สรอ.) แจ้งเวียนหนังสือให้หน่วยงานที่ใช้งาน MailGoThai ทราบว่า จะดำเนินการเปลี่ยนแปลงระบบ MailGoThai (ตามหนังสือ ดศ (สรอ)๕๑๐/๒๕๖๐/ว.๒๒๔๔ ลงวันที่ ๑๗ สิงหาคม ๒๕๖๐) และทรงกรมฯได้ดำเนินการแจ้งเวียนให้กับผู้ใช้งานของกรมฯแล้ว (ตามหนังสือ ทส๐๔๐๒.๕/ว๒๘๖๓ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๐)

#### ๑๔. ปริมาณการใช้งานของอินเทอร์เน็ตภายในกรมฯ

ตั้งแต่วันที่ ๑ สิงหาคม ๒๕๖๒ - ๓๑ สิงหาคม ๒๕๖๒ กรมฯ ใช้อินเทอร์เน็ตแบบ Point-to-point ขนาดความเร็วรวม ๑๒๐/๕๐ Mb/s การใช้งานอินเทอร์เน็ตสูงสุดภายในเดือนสิงหาคม ๒๕๖๒ อยู่ที่ ๙๖.๔๓ Mb/s และค่าเฉลี่ยตลอดทั้งเดือนสิงหาคม ๒๕๖๒ อยู่ที่ ๑๓.๗๓ Mb/s



ปัจจุบัน Internet ทางฝั่ง Inter(ต่างประเทศ) มีปริมาณการใช้งานสูงสุดภายในเดือนสิงหาคม ๒๕๖๒ อยู่ที่ ๓๙.๗๒ Mb/s และค่าเฉลี่ยตลอดทั้งเดือนสิงหาคม ๒๕๖๒ อยู่ที่ ๖.๙๘ Mb/s

ข้อสังเกต หากมีการใช้อินเทอร์เน็ตสูงสุด ๙๕% ของความเร็วอินเทอร์เน็ต ๑๒๐/๕๐ Mb/s ทำให้ความเร็วอินเทอร์เน็ตช้าลง ควรเพิ่มปริมาณ Bandwidth ให้มากขึ้นเป็น ๑๒๐/๖๐ Mb/s เพื่อรองรับปริมาณการใช้งานของ User

## ๑๕. บุคลากร ๑๐ อันดับแรกที่ใช้งานอินเทอร์เน็ตมากที่สุด

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งานอินเทอร์เน็ตของกรมฯ พบบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเทอร์เน็ตมากที่สุด ดังนี้

ลำดับที่	ผู้ใช้งาน	หน่วยงาน	User Name	Data	ตำแหน่ง
๑	วุฒิพงษ์ เพ็ชรไทย	สวพ.	wuttipong.ph	๑๖๔.๕๐ GB	พนักงานราชการ
๒	จรรย์ญา ชนะชัย	สลก.	jarunya.ch	๑๐๘.๔๐ GB	จ้างเหมาบริการ
๓	ไพโรจน์ มาประสบ	สปล.	phairot.ma	๖๗.๔๐ GB	ข้าราชการ
๔	ชนากานต์ สุขอุดม	กผง.	chanakarn.su	๖๒.๓๔ GB	จ้างเหมาบริการ
๕	ภาคากร วิวัฒน์ครุฑ	สสอ.	pakaarkron.wi	๖๐.๖๐ GB	พนักงานราชการ
๖	ณัฐพล บุญยี่น	ศสท.	natapon.bo	๖๐.๓๙ GB	พนักงานราชการ
๗	เสถียร สุเตนนัน	สลก.	sathian.su	๕๗.๘๑ GB	พนักงานราชการ
๘	กรกาญจน์ จรุงแสง	สสอ.	kornkarn.ch	๕๐.๘๙ GB	พนักงานราชการ
๙	รุจรีย์ บัวภิบาล	สลก.	rujaree.bu	๔๙.๒๔ GB	พนักงานราชการ
๑๐	อานนท์ รุจิธรรม	สผต.	anon.ru	๔๔.๒๔ GB	พนักงานราชการ

#	User	Bandwidth
1	wuttipong.ph	164.50 GB
2	JARUNYA.CH	108.40 GB
3	phairot.ma	67.40 GB
4	chanakarn.su	62.34 GB
5	pakaarkron.wi	60.60 GB
6	natapon.bo	60.39 GB
7	sathian.su	57.81 GB
8	kornkarn.ch	50.89 GB
9	Rujaree.bu	49.24 GB
10	anon.ru	44.24 GB

ภาพแสดงบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเทอร์เน็ตมากที่สุดจากระบบ

## ๑๖. Application ใช้งานผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งาน Application ใช้งานผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ ดังนี้

ลำดับที่	Application	Bandwidth
๑	HTTPS	๒.๕๕ TB
๒	Udp/๔๔๓	๙๑๙.๐๔ GB
๓	HTTP	๒๐๖.๒๐ GB
๔	HTTP.BROWSER	๑๗๔.๓๙ GB
๕	SSL	๙๖.๖๐ GB
๖	HTTPS.BROWSER	๖๕.๐๔ GB
๗	Kaspersky Port	๔๗.๑๕ GB
๘	QUIC	๔๐.๕๕ GB
๙	HTTP.Segmented.Download	๓๗.๐๗ GB
๑๐	MS.Windows.Update	๒๔.๙๙ GB

#	Application	Bandwidth	Sent	Received
1	HTTPS			2.55 TB
2	udp/443			919.04 GB
3	HTTP			206.20 GB
4	HTTP.BROWSER			174.39 GB
5	SSL			96.60 GB
6	HTTPS.BROWSER			65.04 GB
7	Kasperky Port			47.15 GB
8	QUIC			40.55 GB
9	HTTP.Segmented.Download			37.07 GB
10	MS.Windows.Update			24.99 GB

ภาพแสดง Application ใช้งานผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

## ๑๗. เครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านอินเทอร์เน็ตมากที่สุด ๑๐ อันดับ

-ไม่พบข้อมูลการโจมตี เนื่องจากมีการติดตั้ง IPS (Intrusion Prevention System) ที่ทำหน้าที่ป้องกันการโจมตีก่อนจะถึง Firewall

## ๑๘. เลขหมายไอพีที่โจมตีผ่านอินเทอร์เน็ต

-ไม่พบการโจมตี เนื่องจากมีการติดตั้ง IPS (Intrusion Prevention System) ที่ทำหน้าที่ป้องกันการโจมตีก่อนจะถึง Firewall

### ๑๙. รายชื่อผู้ใช้งานอินเทอร์เน็ตของกรมฯ ที่มีเวลาการใช้งานมากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงรายชื่อผู้ใช้งานอินเทอร์เน็ตของกรมฯ ที่มีเวลาการใช้งานมากที่สุด ๑๐ อันดับ ดังนี้

ลำดับที่	User Name	ชื่อ-นามสกุล	หน่วยงาน	เวลา(ชั่วโมง)	Bandwidth
๑	๑๐.๑๐.๑๐.๒๓๗	MarineGisCenter	ศสท.	๗๒๓	๑๒.๗๔ GB
๒	srinuna.in (LAN)	ศรีนวล อินทรชิต	สลก.	๑๔๔	๒๑.๔๔ GB
๓	wanee.ou (LAN)	วรรณีย์ อุ่นน้อย	กพง.	๘๙	๑๐.๙๘ GB
๔	๑๐.๑๐.๑๐.๒๔๐	Authen	ศสท.	๗๙	๑.๕๐ GB
๕	paweena.pr (LAN)	ปวีณา พร้อมมงคล	กบช.	๗๔	๓.๐๕ GB
๖	chanokporn.ka (LAN)	ชนกพร กาลรักษา	สทช.	๗๓	๒๘.๗๕ GB
๗	onmaturos.go (LAN)	อรมรุรส โกมาสถิตย์	สลก.	๗๒	๗.๒๙ GB
๘	nawaporn.su (LAN)	นภาพร สุญาณเศรษฐกร	กบช.	๖๗	๑.๗๙ GB
๙	kansud.ke (LAN)	กาญจนาสุดา เกตุดี	สปล.	๖๖	๕.๘๓ GB
๑๐	๑๐.๑๐.๑๐.๒๔๕	Authen	ศสท.	๖๔	๕๒๓.๙๖ MB

#	User (or IP)	Browsing Time(hh:mm:ss)	Bandwidth	Sent	Received
1	10.10.10.237	723:01:16	12.74 GB		
2	srinuna.in	144:05:14	21.44 GB		
3	wanee.ou	89:51:35	10.98 GB		
4	10.10.10.240	79:49:14	1.50 GB		
5	paweena.pr	74:35:00	3.05 GB		
6	chanokporn.ka	73:30:36	28.75 GB		
7	onmaturos.go	72:13:51	7.29 GB		
8	nawaporn.su	67:11:03	1.79 GB		
9	kansud.ke	66:26:01	5.83 GB		
10	10.10.10.245	64:50:24	523.96 MB		

ภาพแสดง รายชื่อผู้ใช้งานอินเทอร์เน็ตของกรมฯ ที่มีเวลาการใช้งานมากที่สุด ๑๐ อันดับ

๒๐. รายชื่อประเทศปลายทางที่ ที่อินเทอร์เน็ตของกรมฯ ได้ทำการติดต่อใช้งานมากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงรายชื่อประเทศปลายทางที่ ที่อินเทอร์เน็ตของกรมฯ ได้ทำการติดต่อใช้งานมากที่สุดมี ดังนี้

ลำดับที่	ประเทศ	Bandwidth
๑	สหรัฐอเมริกา	๒๗๔.๕๒ GB
๒	ไทย	๓.๐๗ TB
๓	สิงคโปร์	๗๔๒.๓๙ GB
๔	เยอรมัน	๑๑.๗๗ GB
๕	Czech Republic	๘๗๓.๑๗ GB
๖	ฮ่องกง	๒๐.๘๗ MB
๗	Malaysia	๑.๑๙ GB
๘	อังกฤษ	๓.๖๘ GB
๙	Netherlands	๘.๔๑ GB
๑๐	Canada	๒.๗๒ GB

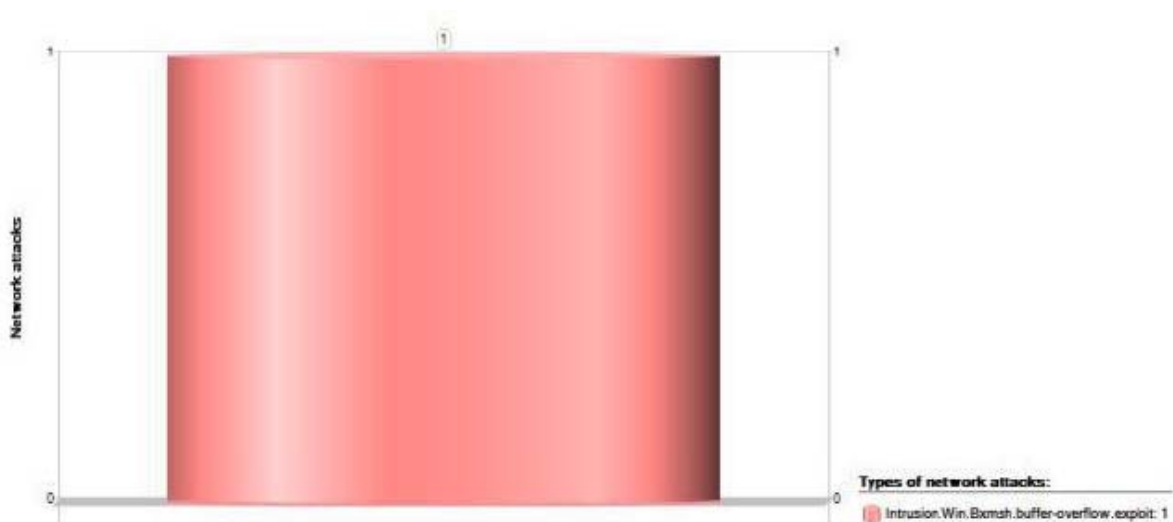
#	Destination	Browsing Time(hh:mm:ss)	Bandwidth	Sent	Received
1	United States	2165:46:59		274.52 GB	
2	Thailand	2135:15:12		3.07 TB	
3	Singapore	710:21:44		742.39 GB	
4	Germany	332:59:59		11.77 GB	
5	Czech Republic	304:06:20		873.17 MB	
6	Hong Kong	248:48:22		20.87 GB	
7	Malaysia	50:56:12		1.19 GB	
8	United Kingdom	38:27:28		3.68 GB	
9	Netherlands	36:08:41		8.41 GB	
10	Canada	30:50:58		2.72 GB	

ภาพแสดง รายชื่อประเทศปลายทางที่ ที่อินเทอร์เน็ตของกรมฯ ได้ทำการติดต่อใช้งานมากที่สุด ๑๐ อันดับ

๒๑. รายชื่อไวรัสที่มีการตรวจจับโดยซอฟต์แวร์ป้องกันไวรัสของกรมฯ มากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบบริหารจัดการซอฟต์แวร์ป้องกันไวรัส (Kaspersky Security Center) แสดงรายชื่อไวรัสที่พบมากที่สุดของระบบเครือข่ายอินเทอร์เน็ตของกรมฯ มีดังนี้

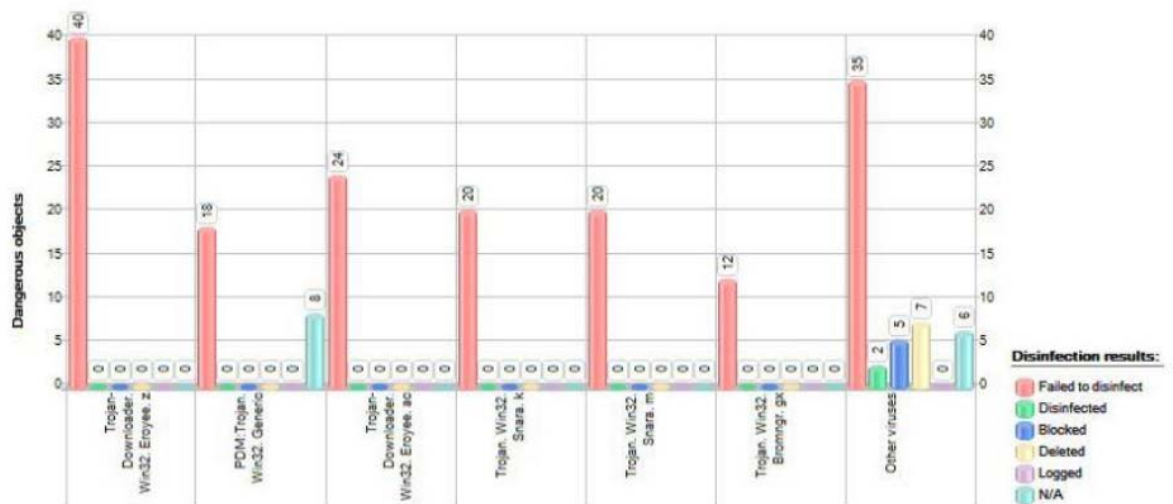
ลำดับที่	รายชื่อไวรัส	จำนวนที่ตรวจจับ
๑	Intrusion.Win.Bxmsh.buffer-overflow.exploit	๑
๒	-	-
๓	-	-
๔	-	-
๕	-	-
๖	-	-
๗	-	-
๘	-	-
๙	-	-
๑๐	-	-



๒๒. รายชื่อไวรัสที่มีการบุกรุกผ่านทางเครือข่ายมากที่สุด ๑๐ อันดับ

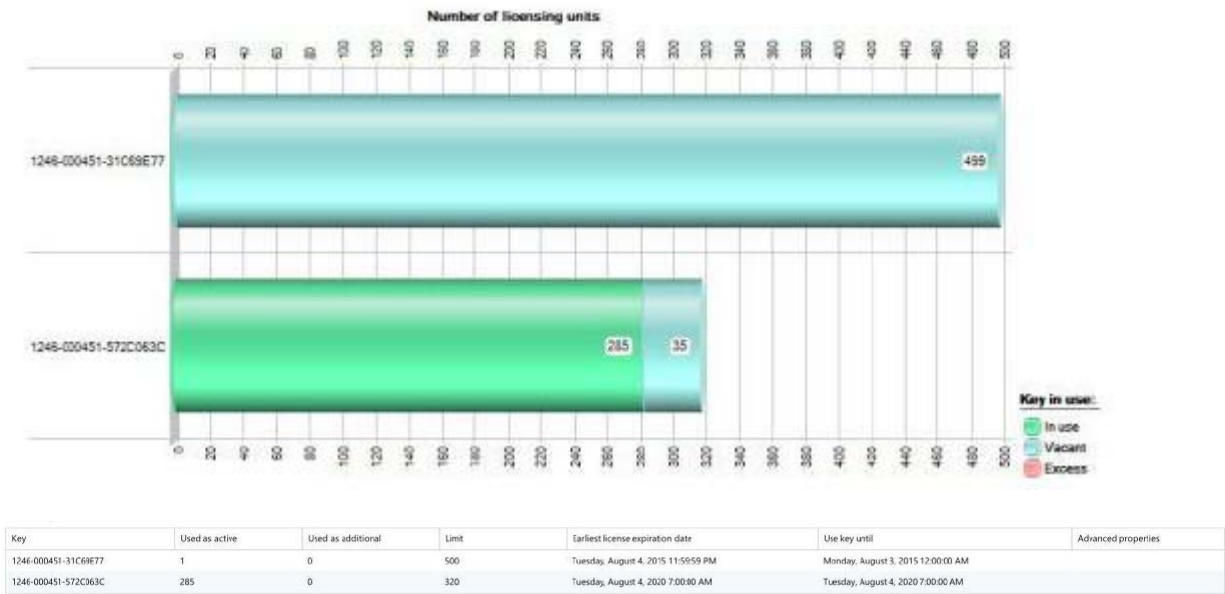
จากการตรวจสอบจากระบบบริหารจัดการซอฟต์แวร์ป้องกันไวรัส (Kaspersky Security Center) แสดงรายชื่อไวรัสที่พบมากที่สุดของผู้ใช้งานระบบเครือข่ายของกรมฯมีดังนี้

ลำดับที่	รายชื่อไวรัส	จำนวนที่ตรวจจับ
๑	Trojan-Downloader.Win๓๒.Eroyee.z	๔๐
๒	PDM:Trojan.Win๓๒.Generic	๒๖
๓	Trojan-Downloader.Win๓๒.Eroyee.ao	๒๔
๔	Trojan.Win๓๒.snara.k	๒๐
๕	Trojan.Win๓๒.snara.m	๒๐
๖	Trojan.Win๓๒.Bromngr.gx	๑๒
๗	Other	๕๕
๘	-	-
๙	-	-
๑๐	-	-





### ๒๓. จำนวนการใช้งานซอฟต์แวร์ป้องกันไวรัส



### ๒๔. การพัฒนาของระบบเครือข่ายที่ผ่านมาระยะที่ ๑

๒๔.๑ ดำเนินการเปลี่ยนอุปกรณ์ป้องกันระบบเครือข่าย (Firewall) เนื่องจากเครื่องเดิมเป็นเครื่องรุ่นเก่าและไม่รองรับจำนวนคนที่เพิ่มขึ้น และระบบมีปัญหาอยู่บ่อยครั้ง จึงมีการจัดซื้อเพื่อเปลี่ยนอุปกรณ์ Firewall จำนวน ๑ เครื่อง เป็นรุ่นที่มีประสิทธิภาพและระบบป้องกันที่ดีมากขึ้น โดยนำมาใช้ป้องกันระบบเครือข่าย LAN และเครื่องคอมพิวเตอร์แม่ข่าย

๒๔.๒ ปรับปรุงระบบเครือข่ายของกรมฯ ให้รองรับทั้ง IPv๔ และ IPv๖

๒๔.๓ ดำเนินการปรับปรุงแบบของ Firewall ตัวเก่าให้นำมาป้องกันการใช้งานระบบ WIFI ซึ่งสามารถรองรับได้ เนื่องจากระบบ WIFI มีคนในกรมฯ ใช้จำนวนน้อย และตัว Firewall ยังสามารถใช้งานได้อยู่

๒๔.๔ การปรับปรุงการใช้งานระบบ Monitor ระบบเครือข่ายกรมฯ เนื่องจากเดิมระบบ Monitor ของกรมฯ ยังเป็นระบบเก่าและไม่สามารถ Update ได้ ในปี ๒๕๖๐ จึงมีการปรับปรุงใหม่ให้มีประสิทธิภาพมากขึ้น โดยสามารถเฝ้าระวังและสังเกตการณ์สิ่งผิดปกติได้ทั้งระบบเครือข่าย

๒๔.๕ ดำเนินการปรับปรุงระบบเครือข่าย โดยเปลี่ยนอุปกรณ์กระจายสัญญาณ (Switch) จากเดิม กรมมี Switch เพียง ๓ เครื่องและเป็นรุ่นเก่า ซึ่งสามารถส่งผ่านหรือโอนถ่ายข้อมูลได้เพียง ๑๐๐ Mbps ทำให้การใช้งานค่อนข้างช้าเกิดเป็นคอขวด ดังนั้นในปี ๒๕๖๐ จึงมีการปรับปรุงระบบใหม่โดยเปลี่ยน Switch และเพิ่มจำนวน ๕ เครื่อง ซึ่งสามารถส่งผ่านหรือโอนถ่ายข้อมูลได้ถึง ๑ Gbps ซึ่งปัญหาคอขวดก็หายไปและยังสามารถแก้ปัญหาในส่วนของการเกิด Loop ซึ่งแต่เดิมที่ยังใช้ Switch รุ่นเก่า นั้นเมื่อเกิด Loop ในระบบ (Loop คือการสถานะที่อุปกรณ์ส่งข้อมูลออกไปบนระบบ แล้วเกิดการวนแบบไม่มีที่สิ้นสุดทำให้ไม่สามารถใช้งาน Internet ได้ ซึ่งเกิดจากการที่ User ต่อสาย LAN ผิด Port ) จะไม่สามารถป้องกันปัญหาได้ทำให้ระบบ Internet ล่มทั้งกรมฯ ซึ่งปัญหาดังกล่าวได้ถูกแก้เมื่อทำการเปลี่ยน Switch ใหม่ แล้วเกิดปัญหา Loop อุปกรณ์สามารถบล็อกให้ปัญหาที่เกิดขึ้นเฉพาะตัวบุคคลไม่ส่งผลกระทบต่อที่ระบบใหญ่ และสามารถสืบหาต้นเหตุได้ทันท่วงที

๒๔.๖ ดำเนินการปรับระบบพิสูจน์ตัวตน (Authentication) ตั้งแต่ปี ๒๕๕๓ มีการใช้ระบบการยืนยันตัวตนแบบ Free Radius บน Linux Server โดยเจ้าหน้าที่ของศูนย์สารสนเทศฯพัฒนาขึ้นมาใช้เอง โดยใช้ชื่ออินเทอร์เน็ตสกอตามด้วยแผนก ตัวอย่าง manee\_PN หมายถึงคนชื่อนี้อยู่กองแผนงาน ซึ่งไม่ค่อยมีความเสถียรและระบบมีปัญหาบ่อยและมีการแอบใช้ User ของคนอื่นเนื่องจากผู้ใช้งาน ๑ คนสามารถ Login เข้าใช้คอมพิวเตอร์ได้หลายเครื่อง ทำให้เกิดปัญหาอื่นๆตามมา และปัญหาเมื่อเวลาที่มีเจ้าหน้าที่ภายในกรมมีการโอน/ย้าย ส่วน/สำนัก/กอง/ศูนย์ ไปมาอยู่บ่อยครั้งซึ่งบางครั้งไม่สามารถแก้ไขเอกสารในการย้ายแผนกได้ เนื่องจากไม่ได้มีการแจ้งข้อมูลให้เจ้าหน้าที่ศูนย์รับทราบ ทำให้เกิดปัญหาข้อมูลซ้ำซ้อนบ้างขอใช้แล้วขอใช้ซ้ำอีกบ้าง จนมาถึงปี ๒๕๖๐ ได้มีแก้ไขปัญหาและการพัฒนาระบบอีกครั้งซึ่งใช้งานแบบกึ่งระบบ AD (Active Directory) โดยการใช้ระบบการพิสูจน์ตัวตนแบบ ใช้ชื่อจุดนามสกุลสองตัวแรก ตัวอย่าง manee.de ซึ่งสามารถแก้ไขปัญหาต่างๆได้ ไม่ว่าจะบุคคลนั้นจะโอน/ย้ายไปไหนก็ตาม ก็ยังคงใช้ชื่อและนามสกุลของบุคคลนั้นได้ตลอด และ User สามารถ Login ใช้งานระบบได้แค่ ๑ User / ๑ อุปกรณ์เท่านั้น กล่าวคือถ้าใช้งานคอมพิวเตอร์เครื่องแรกอยู่ แล้วเกิดต้องการใช้งานคอมพิวเตอร์เครื่องที่ ๒ นั้นต้อง Logout ออกจากเครื่องแรกก่อน ระบบนี้เพื่อป้องกันปัญหาการแอบใช้ User ของบุคคลอื่นในทางที่ผิด รวมถึงการทำ HA ของ Server โดยการนำเครื่องคอมพิวเตอร์แม่ข่าย ๒ เครื่องมาตั้งค่าให้เหมือนกัน และทำงานได้เสมือนว่ามี Server แค่ตัวเดียว ในกรณีที่เมื่อเครื่องใดเครื่องหนึ่งเสียหายจะไม่ส่งผลกระทบต่อการใช้งาน

๒๔.๗ เพิ่มระบบการแจ้งเตือนเมื่อเกิดไฟฟ้าดับ โดยระบบดังกล่าวจะส่ง SMS ไปยังผู้รับผิดชอบ เมื่อเกิดไฟฟ้าดับในห้อง Data Center จำนวน ๕ คน เป็นบริษัทคู่สัญญา ๒ คน และเจ้าหน้าที่กรม ๕ คน

๒๔.๘ เพิ่มระบบสำรองข้อมูล (Backup) เนื่องจากเดิมยังไม่มี Backup ที่เป็นระบบจึงมีการทำระบบขึ้นมาและ Backup เดือนละ ๑ ครั้ง โดยมี ๔ ระบบ ที่ Backup คือ Authen, Anitvirus, e-Tracking, Sarabun และมีการทดสอบการกู้คืนระบบปีละ ๑ ครั้งโดยใช้ระบบ Sarabun ทดสอบซึ่งผลการทดสอบคือสามารถใช้งานได้ปกติ

๒๔.๙ ติดตั้งระบบ IPS (Intrusion Prevention System) ด้วยกรมทรัพยากรทางทะเลและชายฝั่ง โดน Hacker จากภายนอกโจมตีเข้ามาอยู่เป็นประจำและ Firewall ที่ใช้อยู่ไม่สามารถดักจับการโจมตีบางประเภทที่มีความรุนแรงสูง (ทำให้ข้อมูลสูญหาย, Website ถูกทำให้กลายเป็น Web phishing, หรือบางหน้า Website ถูกเปลี่ยนให้เป็น Web ขยายของ) จึงดำเนินการจัดซื้ออุปกรณ์ IPS และปรับตั้งค่าให้สามารถดักจับการโจมตี จนปัจจุบันระบบต่างๆของกรมในห้อง Data Center ไม่มีการพบการถูก Hack หรือโจมตีเข้ามาถึงระบบภายใน แม้กระทั่งตอนที่มัลแวร์ที่หน่วยงานราชการติด Ransomware กรมทรัพยากรทางทะเลและชายฝั่งก็ไม่ถูกโจมตีเข้ามา

๒๔.๑๐ ดำเนินการเปลี่ยน Battery ของ UPS ๑๐ KVA ในห้อง Data Center เนื่องจากเกิดการเสื่อมสภาพเพราะมีอายุการใช้งานยาวนานกว่า ๕ ปี

๒๔.๑๑ จัดหาระบบปฏิบัติการใหม่ เพื่อทดแทนรุ่นเดิมที่ไม่สนับสนุนการทำงานของระบบ

๒๔.๑๒ จัดหาคอมพิวเตอร์แบบพกพา เพื่อทดแทนเครื่องเดิมที่มีอายุการใช้งานหลายปี

## ๒๕. สรุปผลการพัฒนาระบบเครือข่ายระยะที่ ๑

๒๕.๑ เปลี่ยนอุปกรณ์ป้องกันระบบเครือข่าย (Firewall) จากเครื่องเดิม FortiGate ๓๑๐B เป็นเครื่องรุ่น FortiGate ๕๐๐D

๒๕.๒ ดำเนินการปรับปรุงระบบเครือข่ายกรมฯ ที่รองรับ IPv๔ ให้สามารถรองรับทั้ง IPv๔ และ IPv๖ ซึ่งเป็นตัวชี้วัดหนึ่งด้านสารสนเทศของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยทางกรมฯ ได้รับรางวัลรองรับการใช้งาน IPv๖ ๓ ปีติดต่อกันคือปี ๒๕๕๙ ๒๕๖๐ และ ๒๕๖๑ ดังรูป

รายชื่อหน่วยงานที่ให้บริการเครือข่ายอินเทอร์เน็ตพื้นฐานและบริการที่รองรับ IPv6 ติดต่อกัน 3 ปี (หน่วยงานที่ได้รับรางวัลในปี 2015, 2016 และ 2017)

ลำดับ	หน่วยงาน	ปี 2017
1	กรมทรัพยากรทางทะเลและชายฝั่ง	DNS Mail Web DNSSEC
2	กรมบัญชีกลาง	DNS Mail Web DNSSEC
3	การไฟฟ้าส่วนภูมิภาค	DNS Mail Web DNSSEC
4	สำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม	DNS Mail Web DNSSEC
5	สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ	DNS Mail Web DNSSEC
6	สำนักงานคณะกรรมการพัฒนาระบบราชการ	DNS Mail Web DNSSEC
7	สำนักงานคณะกรรมการวิจัยแห่งชาติ	DNS Mail Web DNSSEC
8	สำนักงานบริหารหนี้สาธารณะ	DNS Mail Web DNSSEC
9	สำนักงานปลัดกระทรวงการคลัง	DNS Mail Web DNSSEC
10	สำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์	DNS Mail Web DNSSEC
11	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	DNS Mail Web DNSSEC
12	กรมทรัพย์สินทางปัญญา	DNS Mail Web
13	กรมส่งเสริมการค้าระหว่างประเทศ	DNS Mail Web
14	กรมหมอนไหม	DNS Mail Web
15	สำนักงานเศรษฐกิจการเกษตร	DNS Mail Web
16	สำนักงานเศรษฐกิจการคลัง	DNS Mail Web
17	สำนักเลขาธิการคณะรัฐมนตรี	DNS Mail Web

๒๕.๓ นำ FortiGate ๓๑๐B ซึ่งเป็น Firewall ตัวเก่า มาใช้ในการบริหารจัดการระบบ WiFi

๒๕.๔ ระบบ monitor โดยใช้ cati ในการบริหารจัดการและสังเกตการณ์ระบบเครือข่าย

๒๕.๕ ติดตั้ง Switch Cisco ๓๕๖๐ จำนวน ๕ ตัว ดำเนินการตามสัญญาเลขที่ กพง.๑๓/๒๕๖๐ ลงวันที่ ๓๑ มีนาคม ๒๕๖๐ ติดตั้งเสร็จแล้วเมื่อวันที่ ๒๙ พฤษภาคม ๒๕๖๐

๒๕.๖ ติดตั้งระบบยืนยันตัวตนบุคคลตัวใหม่ (Authentication) เมื่อวันที่ ๒๖ ธันวาคม ๒๕๖๐

๒๕.๗ ติดตั้งระบบแจ้งเตือนเหตุฉุกเฉิน กรณีเกิดไฟฟ้าดับ เมื่อวันที่ ๒๘ ธันวาคม ๒๕๖๐

๒๕.๘ ดำเนินการทำให้ระบบสำรองข้อมูลจำนวน ๔ ระบบ คือ Authen, Anitvirus, e-Tracking, Sarabun เมื่อปี พ.ศ ๒๕๕๙

๒๕.๙ ติดตั้ง IPS ดำเนินการตามสัญญาเลขที่ สลก.๑๑/๒๕๖๐ ลงวันที่ ๒๙ มีนาคม ๒๕๖๐ ติดตั้งแล้วเสร็จเมื่อวันที่ ๓๑ พฤษภาคม ๒๕๖๐

๒๕.๑๐ เปลี่ยน battery เครื่องสำรองไฟ (UPS) เนื่องจากตัวเดิมเสื่อมสภาพจำนวน ๑๖๐ ลูก

๒๕.๑๑ รับมอบ Licenses ระบบปฏิบัติการ Windows ServerSTDCORE ๒๐๑๖ Sngl OLP จำนวน ๓ Licenses

๒๕.๑๒ รับมอบเครื่องคอมพิวเตอร์แบบพกพาหือ Acer จำนวน ๔ เครื่อง ตามสัญญาเลขที่ สลก. ๑๑/๒๕๖๐ เมื่อวันที่ ๒๒ พฤษภาคม ๒๕๖๐

## ๒๖. ปัญหาและอุปสรรค

### ๒๖.๑) ด้านอุปกรณ์/เครื่องคอมพิวเตอร์

๒๖.๑.๑ เครื่องคอมพิวเตอร์และโปรแกรมไม่รองรับเทคโนโลยีปัจจุบันทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

๒๖.๑.๒ ระบบยืนยันตัวตนบุคคล (Authentication) ที่กรมฯใช้ในการบริหารจัดการระบบเครือข่าย ยังเป็นของฟรีทำให้การบริหารจัดการขาดประสิทธิภาพ

๒๖.๑.๓ เครื่องคอมพิวเตอร์แม่ข่าย ล้าสมัยมากแล้ว โดยมีการจัดซื้อตั้งแต่ปี ๒๕๔๙ และ ๒๕๕๑ เป็นจำนวนหลายเครื่อง ซึ่งไม่สามารถที่จะรองรับกับ Application ในปัจจุบัน

### ๒๖.๒) ด้านระบบรักษาความปลอดภัย

๒๖.๒.๑ ไม่สามารถอัปเดต Firmware ของ Fortigate ๕๐๐D ได้ เนื่องจากถ้าอัปเดตแล้ว Fortianalyzer ( ซึ่งเป็นตัวเก็บ Log ) จะไม่สามารถดูผลวิเคราะห์ข้อมูลขั้นสูงได้

### ๒๖.๓) ด้านบริหารจัดการงานเครือข่าย

๒๖.๓.๑ ปัญหาการใช้งาน Internet กรมฯมีปัญหาล่าช้าในบางเวลาเนื่องจากการใช้งาน Website ต่างประเทศ (Inter Traffic) มาก จนทำให้ BandWidth ของกรมฯเต็ม (Internet กรมฯ ความเร็ว ๑๒๐/๕๐ Mb/s โดย ๑๒๐ คือ BandWidth ที่ใช้ภายในประเทศ ส่วน ๕๐ คือ BandWidth ที่ใช้ต่างประเทศ) โดยเรียงลำดับการใช้งาน Website ต่างประเทศ ๕ ลำดับ ดังนี้

- ๑.Windows Update and Other
- ๒.Facebook
- ๓.Google Service (MAP,Cloud,Google Earth,DropBox)
- ๔.Streaming (VDO และสื่อออนไลน์อื่นๆ)
- ๕.Website

๒๖.๓.๒ การติดตั้งโปรแกรม Antivirus ด้วยทางกรมมีการจัดซื้อ Kasperky จำนวน ๓๒๐ Licenses และตั้งค่าให้เกิดประสิทธิภาพในการใช้งานแล้ว แต่ User ส่วนใหญ่มีการถอนการติดตั้ง หรือมีข้อมเครื่องแต่ไม่ได้ติดตั้ง Antivirus เข้าไปใหม่ ปัญหาคือเครื่อง User ที่ไม่ติดตั้ง Antivirus มักจะติดไวรัสทั้งจากอุปกรณ์ มือถือหรือ Flash Drive ที่ติดมากับอุปกรณ์ หรือจากการที่เข้าสู่ Website ที่มีความเสี่ยง ซึ่งต้องคอยแก้ไขปัญหาย่อยบ่อยครั้ง

๒๖.๓.๓ ปัญหาการใช้งาน Internet เกิดจากระบบ Internet ล่ม ซึ่งดูจากข้อมูลและการวิเคราะห์พบว่าปัญหาที่พบตั้งแต่เดือน มกราคม ๒๕๖๑ นั้นเกิดจากผู้ให้บริการ (ISP) ทั้งสิ้น ทั้งจาก CATTELECOM และ TOT ไม่ได้เกิดจากอุปกรณ์ภายในของศูนย์สารสนเทศฯ ซึ่งเป็นปัจจัยที่ควบคุมได้ยาก พอเกิดปัญหาก็โทรแจ้ง

### ๒๖.๔) ด้านบริหารจัดการห้อง Server และอุปกรณ์สำรองไฟ

๒๖.๔.๑ ระบบปรับอากาศภายในห้องกระจายความเย็นไม่ทั่วถึง เนื่องจากมีโต๊ะและกล่องอุปกรณ์อื่นขวางทางลมของระบบ ทำให้บางจุดไม่เย็นและบางจุดความเย็นไม่สม่ำเสมอ

## ๒๗. ข้อเสนอแนะ/แก้ไข

### ๒๗.๑) ด้านอุปกรณ์/เครื่องคอมพิวเตอร์

๒๗.๑.๑ จัดหาคอมพิวเตอร์ที่รองรับเทคโนโลยีปัจจุบัน เนื่องจากภายในกรมฯส่วนใหญ่ยังใช้คอมพิวเตอร์และระบบปฏิบัติการที่เก่าและล้าหลัง ซึ่งบางโปรแกรมไม่รองรับระบบปฏิบัติการแล้ว เช่น Google Chrome ไม่รองรับระบบปฏิบัติการที่เป็น Windows XP และในปีหน้าจะไม่รองรับ Windows ๗

๒๗.๑.๒ จัดหาระบบ AD ที่มี Software ลิขสิทธิ์ รองรับการใช้งาน User ภายในกรมทั้งหมด

๒๗.๑.๓ จัดหาอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายที่มีประสิทธิภาพ และมีการบริหารจัดการที่ยืดหยุ่นมากขึ้น เช่น Blade Server หรือ Hyper Converged Server

### ๒๗.๒) ด้านระบบรักษาความปลอดภัย

๒๗.๒.๑ จัดหา FortiAnalyzer รุ่นที่รองรับกับการทำงาน firmware ของ Fortigate ๕๐๐D รุ่นปัจจุบัน

### ๒๗.๓) ด้านบริหารจัดการงานเครือข่าย

๒๗.๓.๑ กรณีการ Update Windows นั้น ในเบื้องต้นฝ่ายคอมพิวเตอร์และเครือข่าย ดำเนินการเปิดให้ผู้ใช้งาน Update ต่างๆในช่วงเวลา ๑๗.๐๐ น. เป็นต้นไป เพื่อลดปริมาณการใช้ในเวลาราชการ ส่วนการใช้งาน ในลำดับที่ ๒-๕ คือ Website, Facebook, Streaming และ Google Service ได้ดำเนินการบีบช่องสัญญาณให้ลดลง (Shapping Bandwidth) ไว้ และควรเพิ่ม Bandwidth ภายนอกประเทศให้มากขึ้น ประมาณ ๕๐% ของที่ใช้งานอยู่

๒๗.๓.๒ การติดตั้งโปรแกรม Antivirus แก้ปัญหาในเบื้องต้นโดยจะใช้เป็นการออกหนังสือเวียน เป็นคำสั่งหรือนโยบายการใช้งาน ว่าถ้าเครื่องใดไม่ติดตั้ง Antivirus จะไม่แก้ไขปัญหาให้ แต่การแก้ไขแบบถาวรและระยะยาวคือการใช้ระบบ AD ในการควบคุมการติดตั้งและใช้งาน

๒๗.๓.๓ ปัญหาการใช้งาน Internet ตรงส่วนนี้ไม่สามารถแก้ไขปัญหาที่ศูนย์สารสนเทศฯ ได้จึงทำได้เพียงแค่ Monitoring ระบบเครือข่ายและแจ้งไปยัง ISP ผู้ให้บริการให้ดำเนินการแก้ไขปัญหาให้เร็วที่สุด

### ๒๗.๔) ด้านบริหารจัดการห้อง Server และอุปกรณ์สำรองไฟ

๒๗.๔.๑ ปรับเปลี่ยน location ของตู้ RACK และอุปกรณ์อื่นๆ ซึ่งจะดำเนินการในปีงบประมาณถัดไป เนื่องจากว่าต้องมีการวางแผนและจัดเตรียมอุปกรณ์ให้พร้อม

## ๒๘. แนวทางการพัฒนาระบบในอนาคต

๒๘.๑ ปรับปรุงพื้นที่ให้ห้อง Data Center (Re-locate) ปรับเปลี่ยนจุดในการตั้ง Server และอุปกรณ์ภายในใหม่

๒๘.๒ ปรับปรุงระบบ Monitor ให้มีประสิทธิภาพมากขึ้น

๒๘.๓ ปรับปรุงระบบพิสูจน์ตัวตน (Authentication) ให้สามารถบริหารจัดการได้มีประสิทธิภาพมากขึ้น

๒๘.๔ จัดหาระบบ Server ระบบใหม่แบบ Hyper converged ซึ่งมีประสิทธิภาพสูงขึ้นและสามารถรวมระบบและ Application ของทุกหน่วยงานมาไว้ที่ศูนย์สารสนเทศฯ เพื่อง่ายต่อการบริหารจัดการและหน่วยงานไม่ต้องจัดซื้อ Server เองหรือนำไปฝากไว้ที่อื่น เพื่อความปลอดภัยของข้อมูลที่เป็นชั้นความลับ

๒๘.๕ เพิ่มระบบการฝากข้อมูลเรื่องงานที่สำคัญไว้กับศูนย์สารสนเทศฯ

๒๘.๖ รวมการจัดซื้อจัดจ้างระบบ Internet ของกรมฯและต่างจังหวัดเข้าด้วยกัน เพื่อการบูรณาการและการใช้งานข้อมูลระบบที่มีประสิทธิภาพ ปลอดภัยและรวดเร็วมากขึ้นด้วยการใช้ Intranet

๒๘.๗ ปรับปรุงระบบการลงทะเบียนเข้าใช้งาน Internet ทั้ง LAN และ WIFI

๒๘.๘ ปรับปรุงฐานข้อมูลระบบเครือข่ายทั้งหมด

๒๘.๙ ปรับปรุงระบบการ Update Windows โดยการ ใช้ระบบ WSUS เพื่อลดปริมาณ Bandwidth และ Traffic ของอินเทอร์เน็ตกรมฯ เหตุผลความจำเป็นที่ต้องใช้ระบบ WSUS เนื่องจากระบบปฏิบัติการ Windows ในปัจจุบันไม่สามารถปิดการ Update ของ Windows ได้ ซึ่งสาเหตุนี้ทำให้เกิดปัญหาสัญญาณอินเทอร์เน็ตของกรมฯซ้ำ