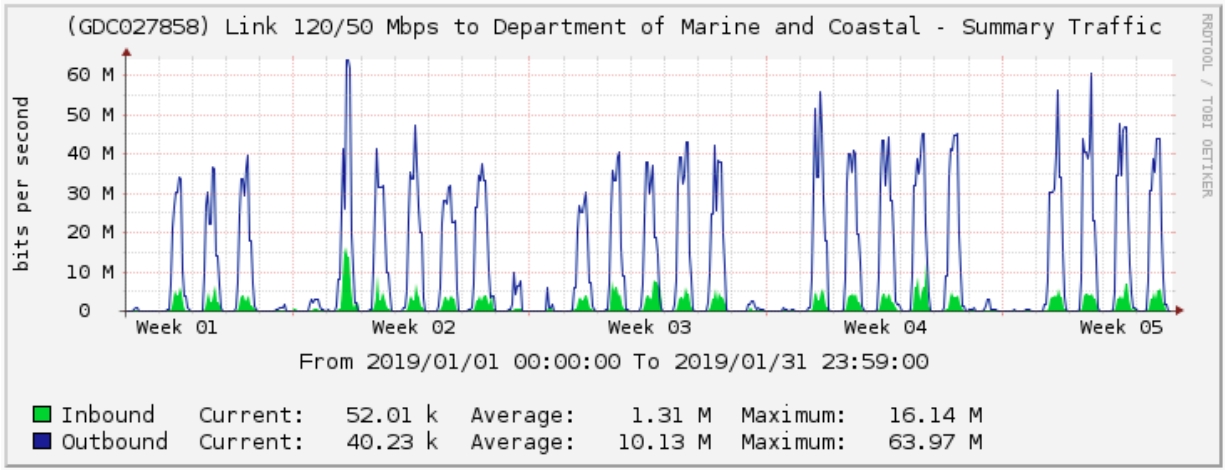
๑๔. ปริมาณการใช้งานของอินเตอร์เน็ตภายในกรมฯ

ตั้งแต่วันที่ ๑ มกราคม ๒๕๖๒ – ๓๑ มกราคม ๒๕๖๒ กรมฯ ใช้อินเตอร์เน็ตแบบ Point-to-point ขนาดความเร็วรวม ๑๒๐/๕๐ Mb/s การใช้งานอินเตอร์เน็ตสูงสุดภายในเดือนมกราคม ๒๕๖๒ อยู่ที่ ๗๒.๗๓ Mb/s และค่าเฉลี่ยตลอดทั้งเดือนมกราคม ๒๕๖๒ อยู่ที่ ๑๒ Mb/s



ปัจจุบัน Internet ทางฝั่ง Inter(ต่างประเทศ) มีปริมาณการใช้งานสูงสุดภายในเดือนมกราคม ๒๕๖๒ อยู่ที่ ๔๙.๕๖ Mb/s และค่าเฉลี่ยตลอดทั้งเดือนมกราคม ๒๕๖๒ อยู่ที่ ๖.๐๔ Mb/s

ข้อสังเกต หากมีการใช้งานอินเตอร์เน็ตสูงสุดใกล้ถึง ๑๑๐/๕๐ Mb/s หรือคิดเป็น ๙๕% ของความเร็วสูงสุดที่สามารถใช้งานได้ ตลอดระยะเวลาที่มีการใช้งาน (เวลา User ใช้งาน) จะมีผลทำให้การใช้งานอินเตอร์เน็ตทั้งหมดช้าลง

๑๕. บุคลากร ๑๐ อันดับแรกที่ใช้งานอินเตอร์เน็ตมากที่สุด

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งานอินเตอร์เน็ตของกรมฯ พบบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเตอร์เน็ตมากที่สุด ดังนี้

ลำดับที่	ผู้ใช้งาน	หน่วยงาน	User Name	Data	ตำแหน่ง
๑	ธิติ้นันท์ เหล่ารอด	สปล.	thitinan.la	๖๙.๙๓ GB	พนักงานราชการ
๒	กรกาญจน์ จรูญแสง	สสอ.	kornkarn.ch	๖๕.๙๐ GB	พนักงานราชการ
๓	ชนากานต์ สุขอุดม	กผง.	chanakarn.su	๕๑.๒๐ GB	จ้างเหมาบริการ
๔	อนุชิต คนแคล้ว	กบช.	anuchit.kh	๕๐.๕๓ GB	ข้าราชการ
๕	ปัทมา ทาสีทอง	สปล.	pattama.ta	๔๗.๕๘ GB	พนักงานราชการ
๖	วันวิสา สาระประไพ	กผง.	vanvisa.sa	๔๔.๙๑ GB	พนักงานราชการ
๗	อุดมศรี อธิเศรษฐ์	สลก.	udomsri.at	๔๒.๗๐ GB	ข้าราชการ
๘	เสถียร สุเตนัน	สลก.	sathian.su	๔๐.๓๖ GB	พนักงานราชการ
๙	๑๙๒.๑๖๘.๑๔.๒๑๓	-	Fortigate๓๑๐B	๓๘.๒๒ GB	-
๑๐	นลินญา สุขพรรณ์	สวพ.	nlinya.su	๓๔.๔๖ GB	พนักงานราชการ

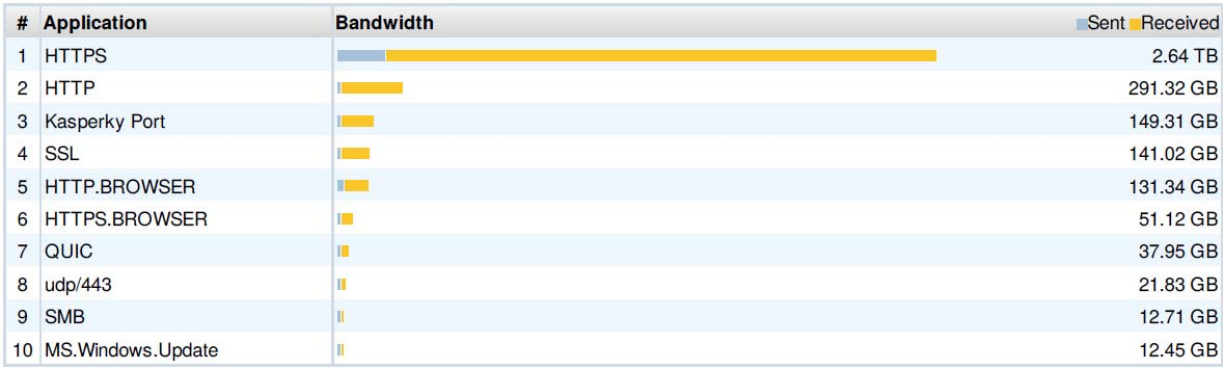
#	User	Bandwidth
1	Thitinan.la	69.93 GB
2	kornkarn.ch	65.90 GB
3	chanakarn.su	51.20 GB
4	anuchit.kh	50.53 GB
5	pattama.ta	47.58 GB
6	Vanvisa.sa	44.91 GB
7	udomsri.at	42.70 GB
8	sathian.su	40.36 GB
9	192.168.14.213	38.22 GB
10	nlinya.su	34.46 GB

ภาพแสดงบุคลากร ๑๐ อันดับแรกที่ใช้งานอินเตอร์เน็ตมากที่สุดจากระบบ

๑๖. Application ใช้งานผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) ในการเข้าใช้งาน Application ใช้งานผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ ดังนี้

ลำดับที่	Application	Bandwidth
๑	HTTPS	๒.๖๔ TB
๒	HTTP	๒๙๑.๓๒ TB
๓	Kaspersky Port	๑๔๙.๓๑ GB
๔	SSL	๑๔๑.๓๑ GB
๕	HTTP.BROWSER	๑๓๑.๓๔ GB
๖	HTTPS.BROWSER	๕๑.๑๒ GB
๗	QUIC	๓๗.๙๕ GB
๘	Udp/๔๔๓	๒๑.๘๓ GB
๙	SMB	๑๒.๗๑ GB
๑๐	MS.Windows.Update	๑๒.๔๕ GB



#	Application	Bandwidth	Sent Received
1	HTTPS		2.64 TB
2	HTTP		291.32 GB
3	Kasperky Port		149.31 GB
4	SSL		141.02 GB
5	HTTP.BROWSER		131.34 GB
6	HTTPS.BROWSER		51.12 GB
7	QUIC		37.95 GB
8	udp/443		21.83 GB
9	SMB		12.71 GB
10	MS.Windows.Update		12.45 GB

ภาพแสดง Application ใช้งานผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับแรกของบุคลากรภายในกรมฯ

๑๗. เครื่องคอมพิวเตอร์ที่ถูกโจมตีผ่านอินเตอร์เน็ตมากที่สุด ๑๐ อันดับ

-ไม่พบข้อมูลการโจมตี เนื่องจากมีการติดตั้ง IPS (Intrusion Prevention System) ที่ทำหน้าที่ป้องกันการโจมตีก่อนจะถึง Firewall

๑๘. เลขหมายไอพีที่โจมตีผ่านอินเตอร์เน็ต

-ไม่พบการโจมตี เนื่องจากมีการติดตั้ง IPS (Intrusion Prevention System) ที่ทำหน้าที่ป้องกันการโจมตีก่อนจะถึง Firewall

๑๙. รายชื่อผู้ใช้งานอินเตอร์เน็ตของกรมฯ ที่มีเวลาการใช้งานมากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงรายชื่อผู้ใช้งานอินเตอร์เน็ตของกรมฯ ที่มีเวลาการใช้งานมากที่สุด ๑๐ อันดับ ดังนี้

ลำดับที่	User Name	ชื่อ-นามสกุล	หน่วยงาน	เวลา(ชั่วโมง)	Bandwidth
๑	๑๐.๑๐.๑๐.๒๓๗	MarineGisCenter	ศสท.	๗๘๒	๑๒.๖๑ GB
๒	๑๐.๑๐.๑๐.๒๔๐	ฐานข้อมูลครุภัณฑ์	ศสท.	๑๒๖	๔๓๒.๔๖ MB
๓	peerapat.sr (LAN)	พีระพัฒน์ ศรีเนาวรัตน์	สปล.	๑๒๐	๑๗.๙๙ GB
๔	paweena.pr (LAN)	ปวีณา พร้อมมงคล	กบช.	๑๑๓	๕.๖๖ GB
๕	chanphen.ch (LAN)	จันทร์เพ็ญ จันทร์ทิม	กผง.	๑๐๒	๑๕.๘๘ GB
๖	srinuna.in (LAN)	ศรีนวล อินทรชิต	สลก.	๙๘	๑๐.๑๓ GB
๗	chanokporn.ka (LAN)	ชนกพร กาลรักษา	สทช.	๘๖	๑๗.๕๑ GB
๘	anuchit.kh (LAN)	อนุชิต คนแคล้ว	กบช.	๘๒	๕๐.๕๐ GB
๙	sopida.kh (LAN)	โสภิดา คำบุญเหลือ	กพร.	๗๖	๒๐.๓๔ GB
๑๐	supadsha.ku (LAN)	สุภัชชา ขุนทอง	กผง.	๖๘	๓.๖๑ GB

#	User (or IP)	Browsing Time(hh:mm:ss)	Bandwidth	Sent Received
1	10.10.10.237	782:09:22		12.61 GB
2	10.10.10.240	126:28:46		432.46 MB
3	peerapat.sr	120:59:18		17.99 GB
4	paweena.pr	113:06:36		5.66 GB
5	chanphen.ch	102:16:18		15.88 GB
6	srinuna.In	98:50:19		10.13 GB
7	chanokporn.ka	86:42:35		17.51 GB
8	anuchit.kh	82:54:40		50.50 GB
9	sopida.kh	76:21:51		20.34 GB
10	supadsha.ku	68:23:43		3.61 GB

ภาพแสดง รายชื่อผู้ใช้งานอินเตอร์เน็ตของกรมฯ ที่มีเวลาการใช้งานมากที่สุด ๑๐ อันดับ

๒๐. รายชื่อประเทศปลายทางที่ ที่อินเตอร์เน็ตของกรมฯ ได้ทำการติดต่อใช้งานมากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (FortiAnalyzer) แสดงรายชื่อประเทศปลายทางที่ ที่อินเตอร์เน็ตของกรมฯ ได้ทำการติดต่อใช้งานมากที่สุดมี ดังนี้

ลำดับที่	ประเทศ	Bandwidth
๑	สหรัฐอเมริกา	๔๐๖.๐๐ GB
๒	ไทย	๒.๒๔ TB
๓	สิงคโปร์	๖๒๒.๕๖ GB
๔	เยอรมัน	๑๕.๙๖ GB
๕	Netherlands	๓๑.๕๓ GB
๖	ฮ่องกง	๑๓.๙๒ GB
๗	Czech Republic	๔๓๑.๘๘ MB
๘	จีน	๓๗๑.๑๕ MB
๙	Japan	๘.๖๑ GB
๑๐	Ireland	๑.๑๙ MB

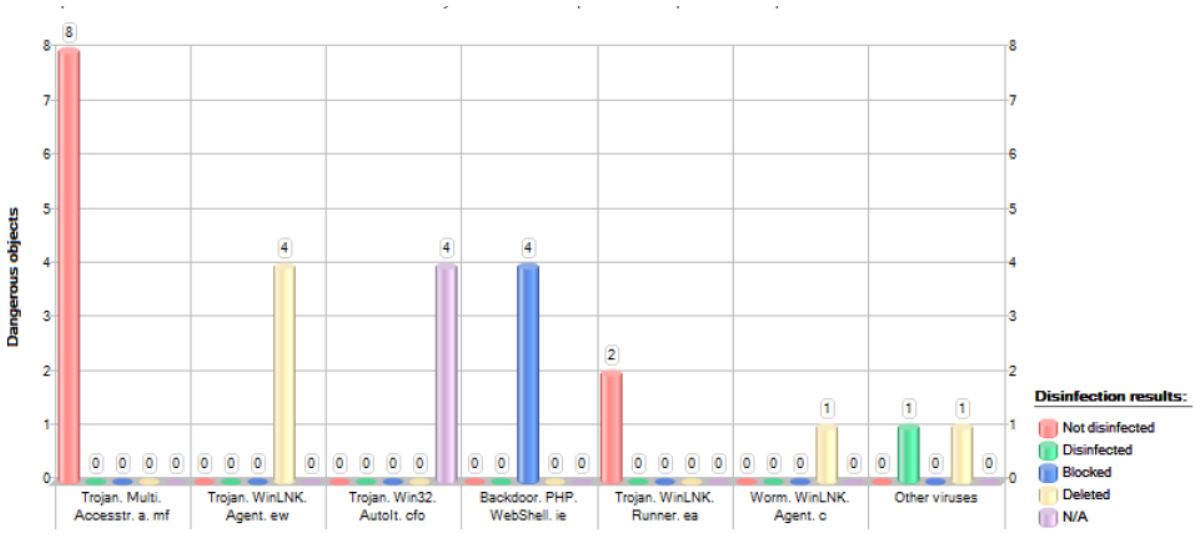
#	Destination	Browsing Time(hh:mm:ss)	Bandwidth	Sent Received
1	United States	2701:51:03		406.00 GB
2	Thailand	2435:07:29		2.24 TB
3	Singapore	724:11:40		622.56 GB
4	Germany	324:41:43		15.96 GB
5	Netherlands	233:55:30		31.53 GB
6	Hong Kong	190:25:07		13.92 GB
7	Czech Republic	56:18:53		431.88 MB
8	China	35:47:50		371.15 MB
9	Japan	33:24:52		8.61 GB
10	Ireland	30:26:37		1.19 GB

ภาพแสดง รายชื่อประเทศปลายทางที่ ที่อินเตอร์เน็ตของกรมฯ ได้ทำการติดต่อใช้งานมากที่สุด ๑๐ อันดับ

๒๑. รายชื่อไวรัสที่มีการตรวจจับโดยซอฟต์แวร์ป้องกันไวรัสของกรมฯ มากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบบริหารจัดการซอฟต์แวร์ป้องกันไวรัส (Kaspersky Security Center) แสดงรายชื่อไวรัสที่พบมากที่สุดของผู้ใช้งานระบบเครือข่ายของกรมฯมีดังนี้

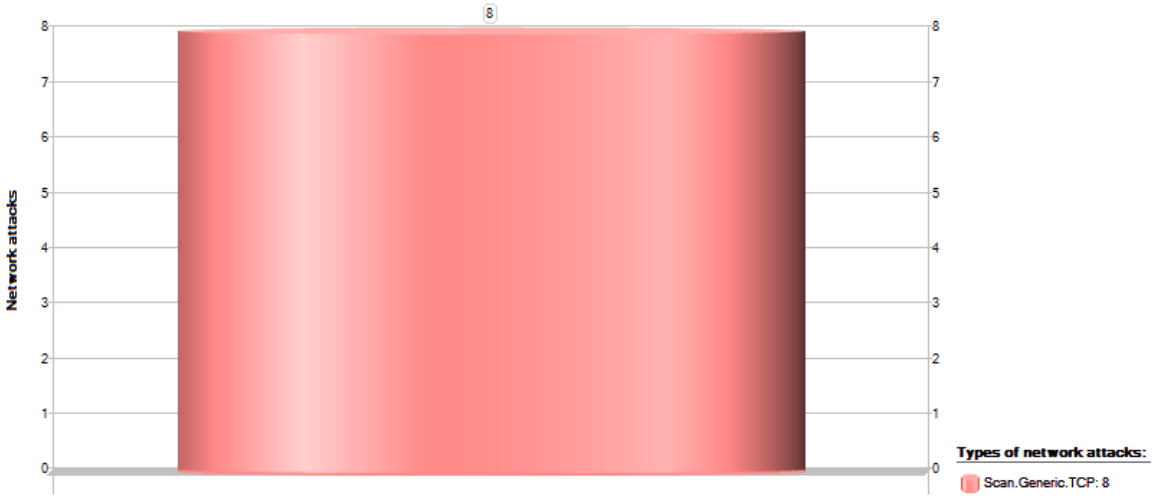
ลำดับที่	รายชื่อไวรัส	จำนวนที่ตรวจจับ
๑	Trojan.Multi.Accesstr.a.mf	๘
๒	Trojan.WinLNK.Agent.ew	๔
๓	Trojan.Win๓๒.Autoit.cfo	๔
๔	Backdoor.PHP.WebShell.ie	๔
๕	Trojan.WinLNK.Runner.ea	๒
๖	Worm.WinLNK.Agent.c	๑
๗	Auther Viruses	๒
๘	-	-
๙	-	-
๑๐	-	-



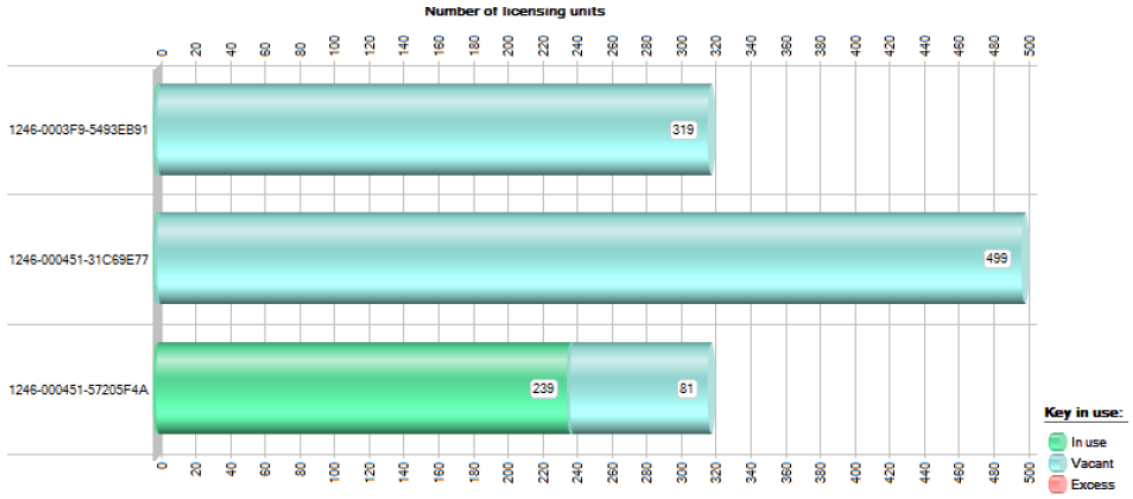
๒๒. รายชื่อไวรัสที่มีการบุกรุกผ่านทางเครือข่ายมากที่สุด ๑๐ อันดับ

จากการตรวจสอบจากระบบบริหารจัดการซอฟต์แวร์ป้องกันไวรัส (Kaspersky Security Center) แสดงรายชื่อไวรัสที่มีการบุกรุกผ่านทางเครือข่ายของกรมฯมีดังนี้

ลำดับที่	รายชื่อไวรัส	จำนวนที่ตรวจจับ
๑	Scan.Generic.TCP	๘
๒	-	-
๓	-	-
๔	-	-
๕	-	-
๖	-	-
๗	-	-
๘	-	-
๙	-	-
๑๐	-	-



๒๓. จำนวนการใช้งานซอฟต์แวร์ป้องกันไวรัส



Summary:

Key	Used as active	Used as additional	Restriction	License expiration date	End date of key validity period	Advanced properties
1246-0003F9-5493EB91	1	0	320	3 สิงหาคม 2561 0:00:00	3 สิงหาคม 2561 0:00:00	Mobile Device Management.
1246-000451-31C69E77	1	0	500	4 สิงหาคม 2558 23:59:59	3 สิงหาคม 2558 0:00:00	
1246-000451-57205F4A	239	0	320	5 สิงหาคม 2562 23:59:59	4 สิงหาคม 2562 0:00:00	

Keys: 3Keys are more than 90% used: 0Keys with exceeded restriction: 0

๒๔. การพัฒนาของระบบเครือข่ายที่ผ่านมาระยะที่ ๑

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

๒๔.๒ ปรับปรุงระบบเครือข่ายของกรมฯให้รองรับทั้ง IPv๔ และ IPv๖

๒๔.๓ ดำเนินการปรับรูปแบบของ Firewall ตัวเก่าให้นำมาป้องกันการใช้งานระบบ WIFI ซึ่งสามารถรองรับได้ เนื่องจากระบบ WIFI มีคนในกรมฯใช้จำนวนน้อย และตัว Firewall ยังสามารถใช้งานได้อยู่

๒๔.๔ การปรับปรุงการใช้งานระบบ Monitor ระบบเครือข่ายกรมฯ เนื่องจากเดิมระบบ Monitor ของกรมฯยังเป็นระบบเก่าและไม่สามารถ Update ได้ ในปี ๒๕๖๐ จึงมีการปรับปรุงใหม่ให้มีประสิทธิภาพมากขึ้น โดยสามารถเฝ้าระวังและสังเกตุการณ์สิ่งผิดปกติได้ทั้งระบบเครือข่าย

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

๒๔.๖ ดำเนินการปรับระบบพิสูจน์ตัวตน (Authentication) ตั้งแต่ปี ๒๕๕๓ มีการใช้ระบบการยืนยันตัวตนแบบ Free Radius บน Linux Server โดยเจ้าที่ของศูนย์สารสนเทศฯพัฒนาขึ้นมาใช้เอง โดยใช้ชื่ออันเดอร์สกอลตามด้วยแผนก ตัวอย่าง manee_PN หมายถึงคนชื่อมานีอยู่กองแผนงาน ซึ่งไม่ค่อยมีความเสถียรและระบบมีปัญหาบ่อยและมีการแอบใช้ User ของคนอื่นเนื่องจากผู้ใช้งาน ๑ คนสามารถ Login เข้าใช้คอมพิวเตอร์ได้หลายเครื่อง ทำให้เกิดปัญหาอื่นๆตามมา และปัญหาเมื่อเวลามีเจ้าหน้าที่ภายในกรมมีการโอน/ย้าย ส่วน/สำนัก/กอง/ศูนย์ ไปมาอยู่บ่อยครั้งซึ่งบางครั้งไม่สามารถแก้ไขเอกสารในการย้านแผนกได้ เนื่องจากไม่ได้มีการแจ้งข้อมูลให้เจ้าหน้าที่ศูนย์รับทราบ ทำให้เกิดปัญหาข้อมูลซ้ำซ้อนบ้างขอใช้แล้วขอใช้ซ้ำอีกบ้าง จนมาถึงปี ๒๕๖๐ ได้มีแก้ไขปัญหาและการพัฒนาระบบอีกครั้งซึ่งใช้งานแบบกึ่งระบบ AD (Active Directory) โดยการใช้ระบบการพิสูจน์ตัวตนแบบ ใช้ชื่อจุดนามสกุลสองตัวแรก ตัวอย่าง manee.de ซึ่งสามารถแก้ไขปัญหาต่างๆได้ ไม่ว่าบุคคลนั้นจะโอน/ย้ายไปไหนก็ตาม ก็จะยังคงใช้ชื่อและนามสกุลของบุคคลนั้นได้ตลอด และ User สามารถ Login ใช้งานระบบได้แค่ ๑ User / ๑ อุปกรณ์เท่านั้น กล่าวคือถ้าใช้งานคอมพิวเตอร์เครื่องแรกอยู่ แล้วเกิดต้องการใช้งานคอมพิวเตอร์เครื่องที่ ๒ นั้นต้อง Logout ออกจากเครื่องแรกก่อน ระบบนี้เพื่อป้องกันปัญหาการแอบใช้ User ของบุคคลอื่นๆในทางที่ผิด รวมถึงการทำ HA ของ Server โดยการการนำเครื่องคอมพิวเตอร์แม่ข่าย ๒ เครื่องมาตั้งค่าให้เหมือนกัน และทำงานได้เสมือนว่ามี Server แค่ตัวเดียว ในกรณีที่เมื่อเครื่องใดเครื่องหนึ่งเสียหายจะไม่ส่งผลต่อการให้บริการ

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

๒๔.๘ เพิ่มระบบสำรองข้อมูล (Backup) เนื่องจากเดิมยังไม่มีการ 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 ที่ใช้อยู่นั้นไม่สามารถดักจับการโจมตีบางประเภทที่มีความรุนแรงสูง (ทำให้ข้อมูลสูญหาย, Website ถูกทำให้กลายเป็น Web phishing, หรือบางหน้า Website ถูกเปลี่ยนให้เป็น Web ขายของ) จึงดำเนินการจัดซื้ออุปกรณ์ IPS และปรับตั้งค่าให้สามารถดักจับการโจมตี จนปัจจุบันระบบต่างๆของกรมในห้อง Data Center ไม่มีการพบการถูก Hack หรือโจมตีเข้ามาถึงระบบภายใน แม้กระทั่งตอนที่มีข่าวการที่หน่วยงานราชการติด Ransomware กรมทรัพยากรทางทะเลและชายฝั่งก็ไม่ถูกโจมตีเข้ามา

๒๔.๑๐ ดำเนินการเปลี่ยน Battery ของ UPS ๑๐ KVA ในห้อง Data Center เนื่องจากเกิดการเสื่อมสภาพเพราะมีอายุการใช้นานยาวนานกว่า 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 โดยทางกรมฯได้รับรางวัลรองรับการใช้งาน 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	กรมหม่อนไหม	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 ในการบริหารจัดการและสังเกตุการณ์ระบบเครือข่าย

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

๒๕.๖ ติดตั้งระบบยืนยันตัวบุคคลตัวใหม่ (Authentication) เมื่อวันที่ ๒๖ ธันวาคม ๒๕๖๐

๒๕.๗ ติดตั้งระบบแจ้งเตือนเหตุฉุกเฉิน กรณีเกิดไฟฟ้าดับ เมื่อวันที่ ๒๘ ธันวาคม ๒๕๖๐

๒๕.๘ ดำเนินการทำระบบสำรองข้อมูลจำนวน 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 รับมอบเครื่องคอมพิวเตอร์แบบพกพายี่ห้อ Acer จำนวน ๔ เครื่อง ตามสัญญาเลขที่ สลก. ๑๑/๒๕๖๐ เมื่อวันที่ ๒๒ พฤษภาคม ๒๕๖๐

๒๖. ปัญหาและอุปสรรค

๒๖.๑) <u>ด้านอุปกรณ์/เครื่องคอมพิวเตอร์</u>

๒๖.๑.๑ เครื่องคอมพิวเตอร์และโปรแกรมไม่รองรับเทคโนโลยีปัจจุบันทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

๒๖.๑.๒ ระบบยืนยันตัวบุคคล (Authentication) ที่กรมฯใช้ในการบริหารจัดการระบบเครือข่าย ยังเป็นของฟรีทำให้การบริหารจัดการขาดประสิทธิภาพ

๒๖.๑.๓ เครื่องคอมพิวเตอร์แม่ข่าย ล้าสมัยมากแล้ว โดยมีการจัดซื้อตั้งแต่ปี ๒๕๔๙ และ ๒๕๕๑ เป็นจำนวนหลายเครื่อง ซึ่งไม่สามารถที่จะรองรับกับ Application ในปัจจุบัน

๒๖.๒) <u>ด้านระบบรักษาความปลอดภัย</u>

๒๖.๒.๑ ไม่สามารถอัพเดท Firmware ของ Fortigate ๕๐๐D ได้ เนื่องจากถ้าอัพเดทแล้ว Fotianalyzer (ซึ่งเป็นตัวเก็บ Log) จะไม่สามารถดูผลวิเคราะห์ข้อมูลขั้นสูงได้

๒๖.๓) <u>ด้านบริหารจัดการงานเครือข่าย</u>

๒๖.๓.๑ ปัญหาการใช้งาน Internet กรมฯมีปัญหาล่าช้าในบางเวลาเนื่องจากมีการใช้งาน 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 และสื่ออนไลน์อื่นๆ)

๕.Website

๒๖.๓.๒ การติดตั้งโปรแกรม Antivirus ด้วยทางกรมมีการจัดซื้อ Kasperky จำนวน ๓๒๐ Licenses และตั้งค่าให้เกิดประสิทธิภาพในการใช้งานแล้ว แต่ User ส่วนใหญ่มีการถอนการติดตั้ง หรือมีซ่อมเครื่องแต่ไม่ได้ติดตั้ง Antivirus เข้าไปใหม่ ปัญหาคือเครื่อง User ที่ไม่ติดตั้ง Antivirus มักจะติดไวรัสทั้งจากอุปกรณ์ มือถือหรือ Flash Drive ที่ติดมากับอุปกรณ์ หรือจากการที่เข้าดู Website ที่มีความเสี่ยง ซึ่งต้องคอยแก้ไขปัญหาอยู่บ่อยครั้ง

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

๒๖.๔) <u>ด้านบริหารจัดการห้อง Server และอุปกรณ์สำรองไฟ</u>

๒๖.๔.๑ ระบบปรับอากาศภายในห้องกระจายความเย็นไม่ทั่วถึง เนื่องจากมีโต๊ะและกล่องอุปกรณ์อื่นขวางทางลมของระบบ ทำให้บางจุดไม่เย็นและบางจุดความเย็นไม่สม่ำเสมอ

๒๗. ข้อเสนอแนะ/แก้ไข

๒๗.๑) <u>ด้านอุปกรณ์/เครื่องคอมพิวเตอร์</u>

๒๗.๑.๑ จัดหาคอมพิวเตอร์ที่รองรับเทคโนโลยีปัจจุบัน เนื่องจากภายในกรมฯส่วนใหญ่ยังใช้คอมพิวเตอร์และระบบปฏิบัติการที่เก่าและล้าหลัง ซึ่งบางโปรแกรมไม่รอบรับระบบปฏิบัติการแล้ว เช่น Google Chome 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) <u>ด้านระบบรักษาความปลอดภัย</u>

๒๗.๒.๑ จัดหา FortiAnalyzer รุ่นที่รองรับกับการทำงาน firmware ของ Fotigate ๕๐๐D รุ่นปัจจุบัน

๒๗.๓) <u>ด้านบริหารจัดการงานเครือข่าย</u>

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 ภายนอกประเทศให้มากขึ้นประมาณ 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 ผู้ให้บริการให้ดำเนินการแก้ปัญหาให้เร็วที่สุด

๒๗.๔) <u>ด้านบริหารจัดการห้อง Server และอุปกรณ์สำรองไฟ</u>

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 ปรับปรุงระบบพิสูนจ์ตัวตน (Authentication) ให้สามารถบริหารจัดการได้มีประสิทธิภาพมากขึ้น

๒๘.๔ จัดหาระบบ Server ระบบใหม่แบบ Hyper converged ซึ่งมีประสิทธิภาพสูงขึ้นและสามารถรวมระบบและ Application ของทุกหน่วยงานมาไว้ที่ศูนย์สาสนเทศฯ 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 โดยการใช้ระบบ WSUS เพื่อลดปริมาณ Banwidth และ Traffic ของอินเตอร์เน็ตกรมฯ เหตุผลความจำเป็นที่ต้องใช้ระบบ WSUS เนื่องจากระบบปฏิบัติการ Windows ในปัจจุบันไม่สามารถปิดการ Update ของ Windows ได้ ซึ่งสาเหตุนี้ทำให้เกิดปัญหาสัญญาณอินเตอร์เน็ตของกรมฯช้า