กรมการปกครอง กระทรวงมหาดไทย
Department Of Provincial Administration

โครงการเช่าระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศกรมการปกครอง (Security Operations Center: SOC)

งบประมาณประจำปี พ.ศ. 2566

- จำนวนเงินทั้งสิ้น 948,359,900 บาท
- ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์ 381,674,816.37 บาท

1. วัตถุประสงค์โครงการ

1. เพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของข้อมูลต่าง ๆ ที่กรมการปกครองจัดเก็บ
2. เพื่อเพิ่มประสิทธิภาพให้กับโครงข่ายระบบสารสนเทศของกรมการปกครอง ให้มีความเสถียรภาพมากขึ้น
3. เพื่อเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามทางไซเบอร์

2. เป้าหมาย

1. ติดตั้งระบบคอมพิวเตอร์ส่วนกลาง 2 แห่ง ประกอบด้วย
   สำนักบริหารการทะเบียน คลองเก้า อำเภอลำลูกกา จังหวัดปทุมธานี และ วังไชยา นางเลิ้ง กรุงเทพมหานคร
2. ติดตั้งซอฟต์แวร์ระบบเพื่อป้องกัน , ตรวจจับ และบริหารจัดการคอมพิวเตอร์ส่วนภูมิภาคทั่วประเทศ

3. ประโยชน์ที่คาดว่าจะได้รับ

1. ข้อมูลของประชาชนที่กรมการปกครองจัดเก็บ มีความปลอดภัยมากยิ่งขึ้น
2. ระบบมีความปลอดภัยมากยิ่งขึ้น เพราะมีการเฝ้าระวังตลอด 24 ชั่วโมง
3. ลดความเสียหายที่จะเกิดขึ้น เพราะรู้ทันทีเมื่อถูกโจมตี ทำให้สามารถแก้ไขปัญหาได้รวดเร็ว
4. สามารถแก้ไขปัญหาได้ที่ต้นเหตุ มีการตรวจสอบความผิดปกติในระดับเชิงลึกเพื่อปิดช่องโหว่

อ้างอิงตามมาตรฐาน Cybersecurity Framework | NIST

The National Institute of Standards and Technology (NIST)

NIST Cyber Security Framework		รายการที่จัดหา
Identify	การระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง	ซอฟต์แวร์ระบบบริหารจัดการช่องโหว่ด้านความปลอดภัยระบบสารสนเทศ (Vulnerability Assessment and Penetration Testing)
		ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร
		อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย Network access control (NAC)
		ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง
		ระบบป้องกันภัยคุกคามโดยกลยุทธ์ (Deception Solution)
Protect	การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร	ระบบบริหารจัดการทรัพยากรบนเครือข่าย (Active Directory)
		อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
		ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR)
		อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)
		อุปกรณ์บริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)
		อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร
		อุปกรณ์ป้องกันและรักษาความปลอดภัยภัยระบบชื่อโดเมน (DNS Firewall) และ โดเมนภายในองค์กร (DNS Security)
Detect	การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ	ระบบจัดเก็บข้อมูลและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)
		อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง fortiSandbox
		อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ fortiAI
Respond	การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูล ระบบเครือข่าย fortianlzer
Recovery	การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม	ห้องปฏิบัติการ Security Operations Center (SOC)
		SOC TIER 1 Services Operator 24x7.

Identify : การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง

1. ซอฟต์แวร์ระบบบริหารจัดการช่องโหว่ด้านความปลอดภัยระบบสารสนเทศ (Vulnerability Assessment and Penetration Testing) จำนวน 1 ระบบ
   - ซอฟต์แวร์ตรวจสอบช่องโหว่ (Vulnerability Assessment)
   - ซอฟต์แวร์ทดสอบการเจาะระบบเครือข่ายคอมพิวเตอร์ (Penetration Testing)

2. ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข5ายภายในองค์กร (Network performance monitor) จำนวน 1 ระบบ
   - ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่าย
   - ซอฟต์แวร์วิเคราะห์ Traffic ที่เกิดขึ้นภายในระบบเครือข่าย

3. อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network access control) จำนวน 2 หน่วย

4. ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) จำนวน 12,500 ชุด

5. ระบบป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) จำนวน 1 ระบบ
   - ระบบตรวจจับภัยคุกคามทางไซเบอร์บนระบบเครือข่ายด้วยการวางกับดักและเหยื่อล่อ (Deception)
   - ระบบการวางเหยื่อล่อ (Baits, Breadcrumb) บนเครื่องผู้ใช้งานหรือเครื่องแม่ข่าย และป้องกันข้อมูลจาก Ransomware ร่วมกับระบบวางกับดัก

Protect : การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร

1. ระบบบริหารจัดการทรัพยากรบนเครือข่าย (Active Directory) จำนวน 12,500 ชุด

2. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน 4 หน่วย

3. ระบบปล้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response) จำนวน 12,500 ชุด

4. อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway) จำนวน 2 หน่วย

5. ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management) จำนวน 1 ระบบ

6. อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection) จำนวน 4 หน่วย

7. ระบบป้องกันและรักษาความปลอดภัยภัยระบบชื่อโดเมน (DNS Firewall) และ โดเมนภายในองค์กร (DNS Security)

NIST Cyber Security Framework

Detect : การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ

1. ระบบจัดเก็บข้อมูลและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)
   - ระบบเก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่าย (LOG)
   - ระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)

2. อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง จำนวน 1 หน่วย

3. อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ จำนวน 1 หน่วย

Respond : การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

1. อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย จำนวน 1 หน่วย

Recovery : การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

1. ห้องปฏิบัติการ Security Operations Center (SOC)
2. SOC TIER 1 Services Operator 24x7

รายการอุปกรณ์คอมพิวเตอร์ที่ขออนุมัติ (กรณีไม่ตรงตามเกณฑ์)

ลำดับ	รายการ	จำนวนที่จัดหา	ราคาต่อหน่วย	รวมเงินทั้งสิ้น
1	ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment)	1	1,372,000	1,372,000
2	ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor)	1	350,000	350,000
3	อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network access control)	2	1,500,000	3,000,000
4	ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software)	11,500	850	9,775,000
5	อุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) พร้อม software Network Detection 200 สิทธิ์	2	15,587,200	31,174,400
6	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	4	5,599,600	22,398,400
7	ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response)	11,500	3,360	38,640,000
8	อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)	2	1,195,300	2,390,600
9	ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)	1	37,270,816.37	37,270,816.37
10	อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection)	4	5,981,725	23,926,900
11	ระบบป้องกันภัยคุกคาม Domain Name System	500	3,800	1,900,000

รายการอุปกรณ์คอมพิวเตอร์ที่ขออนุมัติ (กรณีไม่ตรงตามเกณฑ์)

ลำดับ	รายการ	จำนวนที่จัดหา	ราคาต่อหน่วย	รวมเงินทั้งสิ้น
12	ระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)	1	28,500,000	28,500,000
13	อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง	1	9,700,000	9,700,000
14	อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์	1	15,796,000	15,796,000
15	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย	1	5,679,900	5,679,900
16	ลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) บนอุปกรณ์ Internet Proxy Gateway	1,000	4,500	4,500,000
17	ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone	2	1,780,000	3,560,000
18	อุปกรณ์ป้องกันเครือข่าย Internet Firewall	4	22,338,000	89,352,000
19	อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application ระหว่างศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า-นางเลิ้ง	4	8,850,000	35,400,000
20	ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network)	2	2,196,400	4,392,800
21	อุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch	4	1,994,000	7,976,000
22	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง	4	1,155,000	4,620,000
	รวมจำนวนเงินกรณีไม่ตรงตามเกณฑ์			**381,674,816.37**
	รวมจำนวนเงินในส่วนที่เป็นอุปกรณ์คอมพิวเตอร์			**381,674,816.37**

รายการอุปกรณ์คอมพิวเตอร์ที่ขออนุมัติ (อื่น ๆ)

ลำดับ	รายการ	จำนวนที่จัดหา	ราคาต่อหน่วย	รวมเงินทั้งสิ้น
1	ห้องปฏิบัติการ Security Operations Center (SOC)	1	2,500,000	2,500,000
2	SOC Services Operators 24x7 ระยะเวลา 12 เดือน	12	900,000	10,800,000
3	ค่า Implement Setup and Configuration สำหรับศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า-นางเลิ้ง	1	9,000,000	9,000,000
	รวมจำนวนเงินที่เป็นอุปกรณ์อื่น ๆ			22,300,000

มูลค่าสินค้าทั้งหมด เป็นจำนวนเงิน 403,974,816.37 บาท

งบประมาณ

งบประมาณประจำปี	จำนวนเงิน (บาท)
2566	58,482,190
2567	139,092,780
2568	158,059,980
2569	158,059,980
2570	158,059,980
2571	158,059,980
2572	118,545,010
รวม	**948,359,900**

มูลค่าสินค้าทั้งหมด เป็นจำนวนเงิน 403,974,816.37 บาท

มูลค่าบำรุงรักษา ระยะเวลา 5 ปี เป็นจำนวนเงิน 489,981,950 บาท

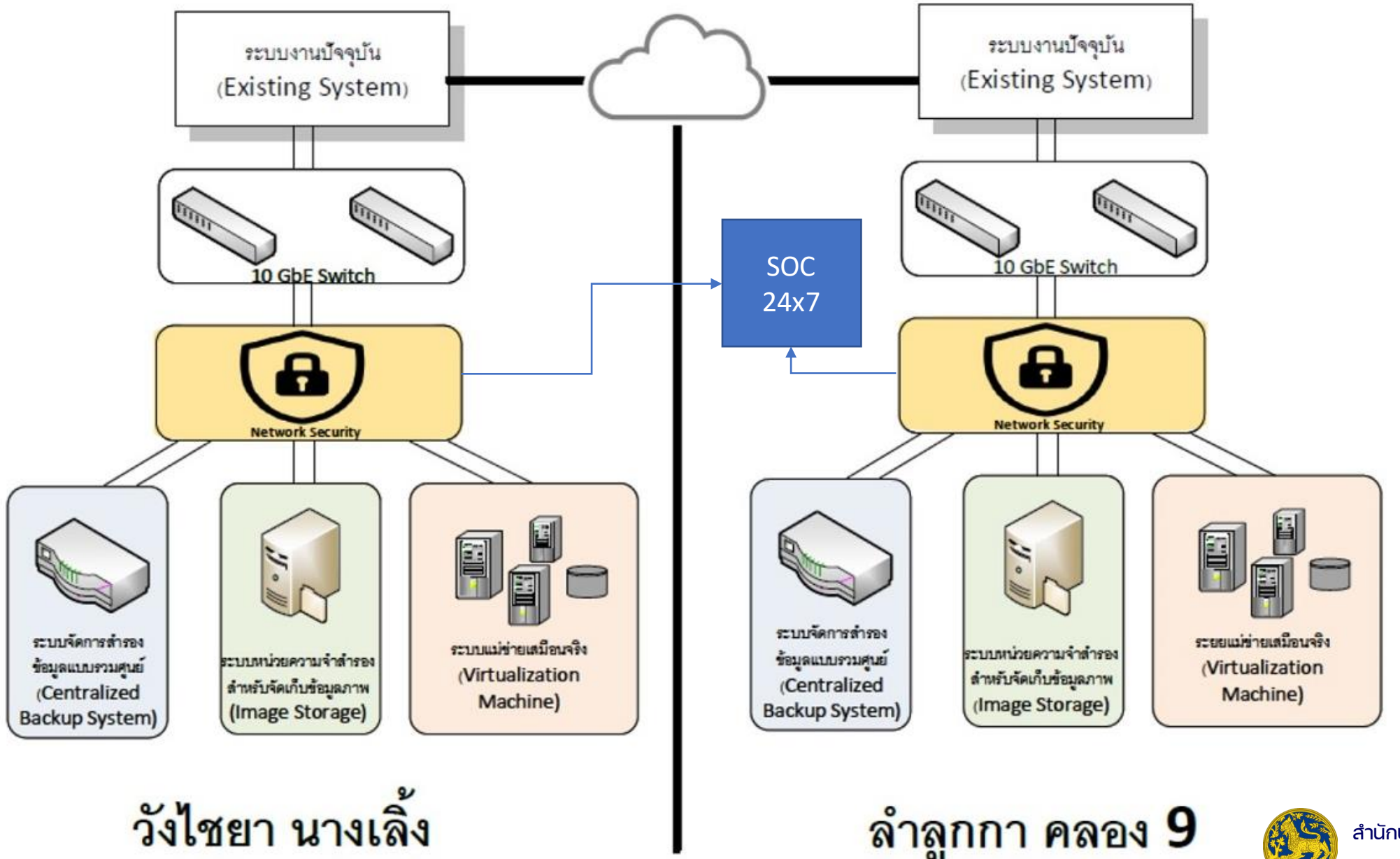
มูลค่าดอกเบี้ย ระยะเวลา 6 ปี เป็นจำนวนเงิน 54,404,554.69 บาท

รวมเป็นเงินค่าเช่าทั้งโครงการ จำนวน 948,359,900 บาท

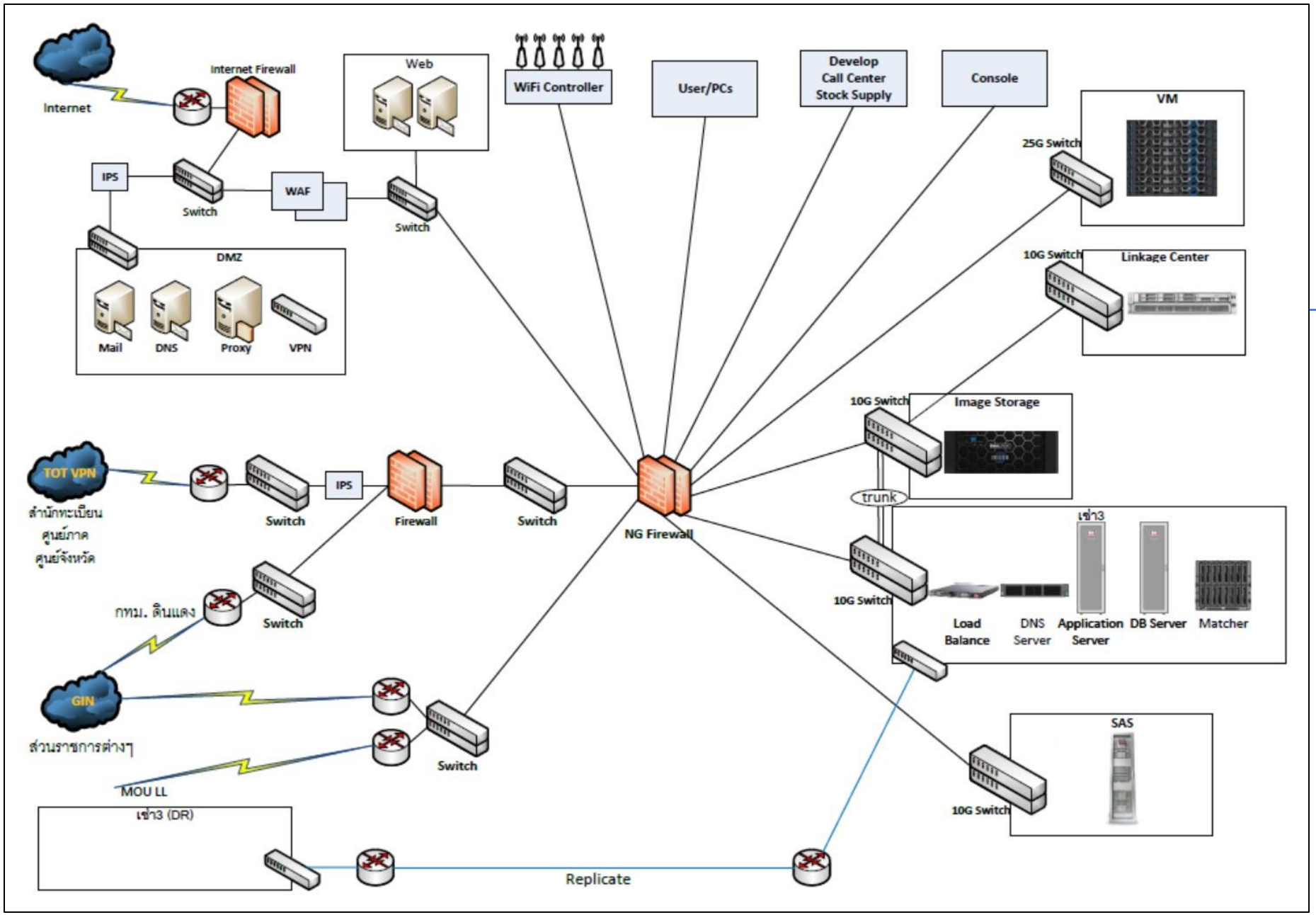
ตั้งแต่ปีที่ 2 – 6 คิดค่าบำรุงรักษา ต่อปี (MA Hardware + Software license Subscription per year)
เป็นจำนวนเงิน 97,996,390 บาท/ปี (ไม่รวมดอกเบี้ย)

ค่าดอกเบี้ย (อัตรา MLR-1 = 4.25) ณ วันที่ 11 ต.ค. 2564
มูลค่าดอกเบี้ย ระยะเวลา 6 ปี เป็นจำนวนเงิน 54,404,554.69 บาท

แผนผังการเชื่อมโยงระบบ



แผนผังการเชื่อมโยงระบบ



SIEM

สำนักบริหารการทะเบียน
กรมการปกครอง

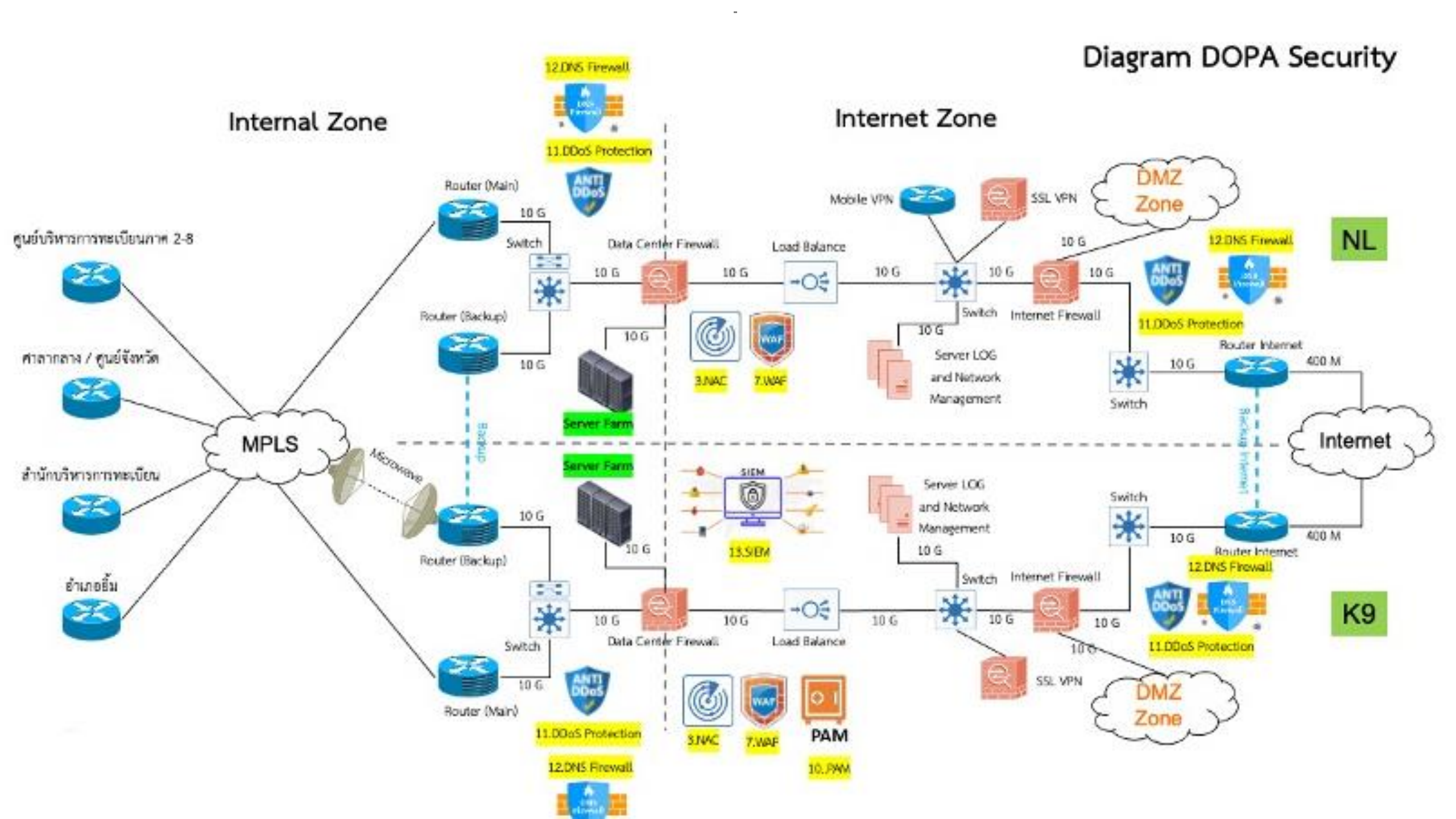


Diagram DOPA Security
Internal Zone
Internet Zone
12.DNS Firewall
11.DDoS Protection
Router (Main)
10 G
Switch
Data Center Firewall
Load Balance
Mobile VPN
SSL VPN
DMZ Zone
NL
ศูนย์บริหารการทะเบียนกลาง 2-8
ศาลากลาง / ศูนย์จังหวัด
สำนักบริหารการทะเบียน
อำเภอยิ้ม
Router (Backup)
MPLS
Microwave
Server Farm
3.NAC
7.WAF
Server LOG and Network Management
Internet Firewall
Router Internet
400 M
Internet
SIEM
13.SIEM
PAM
10.PAM
K9

ระยะเวลาดำเนินการ

กิจกรรม	2565			2566											หมายเหตุ
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	
1. ขออนุมัติโครงการ															
2. ดำเนินการจัดหาระบบคอมพิวเตอร์															
3. ลงนามในสัญญา															
4. ติดตั้ง/ส่งมอบระบบคอมพิวเตอร์															
5. ทดสอบ/ตรวจรับระบบคอมพิวเตอร์															

ระยะเวลาดำเนินงานโครงการ 180 วัน

ข้อสังเกตและข้อเสนอแนะของคณะทำงานฯ

1. ให้แสดงเหตุผลความจำเป็นในการเช่าแทนการจัดซื้อ และระบุผลการศึกษาวิเคราะห์ถึงความคุ้มค่าในการลงทุนด้วยการเช่าแทนการจัดซื้อให้ชัดเจน

2. ทุกหน่วยงานไม่จำเป็นต้องมีศูนย์ SOC เป็นของตัวเอง ในกรณีเป็นหน่วยงานที่มีขนาดเล็ก จะไม่มีงบประมาณในการสร้างศูนย์ SOC ของหน่วยงานได้ แต่หาก สป.มท. สามารถดำเนินการสร้างศูนย์ SOC กลางได้ ก็จะสามารถลดค่าใช้จ่ายในภาพรวมของ มท.

จึงเรียนมาเพื่อโปรดพิจารณา