เอกสารนำเสนอ

คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์
ของกรมการปกครอง

โครงการเช่าระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ
(Security Operations Center: SOC)

งบประมาณรายจ่ายประจำปี 2566 จำนวนเงิน 948,359,900 บาท

กรมการปกครอง

สารบัญ

	หน้า
ก. ข้อมูลทั่วไป	**1**
1. ชื่อโครงการ	1
2. ส่วนราชการ	1
3. วงเงินงบประมาณ	1
4. สัดส่วนของงบประมาณ	2
5. การพิจารณาของคณะกรรมการบริหารและจัดหาระบบคอมฯ	2
6. ความสอดคล้องกับยุทธศาสตร์ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม	2
ข. ข้อมูลโครงการ	**3**
1. หลักการและเหตุผลความเป็นมา	3
2. วัตถุประสงค์	3
3. เป้าหมาย	3
4. โครงการที่จัดหาครั้งนี้ เป็นการที่จัดหาใหม่หรือทดแทนระบบเดิม	3
5. สภาพปัจจุบัน	4
5.1 สถานภาพระบบคอมพิวเตอร์ปัจจุบัน	4
5.2 สภาพปัญหา	4
5.3 ระบบหรืออุปกรณ์ที่มีอยู่ในปัจจุบันของหน่วยงาน	4
6. ระบบงานและปริมาณงานที่จะดำเนินการ	8
6.1 ความแตกต่างของระบบเดิมกับระบบใหม่	8
6.2 ลักษณะและปริมาณงาน	9
6.3 ระบบงานและวิธีการนำเข้าข้อมูล	10
7. สถาปัตยกรรมการจัดการองค์กร (Enterprise Architecture)	10
7.1 สถาปัตยกรรมการจัดการองค์กรด้านพันธกิจ	10
7.2 สถาปัตยกรรมการจัดการองค์กรด้านระบบสารสนเทศ	11
7.3 สถาปัตยกรรมการจัดการองค์กรด้านข้อมูล	12
7.4 สถาปัตยกรรมการจัดการองค์กรด้านเทคโนโลยี	12
8. รายการที่จะจัดหา	17
9. สถานที่ติดตั้งใช้งานระบบ / อุปกรณ์	19
10. การฝึกอบรม	20
11. ระยะเวลาดำเนินงาน	20
12. ผลผลิตของโครงการ	20
13. ตัวชี้วัดสัมฤทธิ์ผลด้าน IT	20
14. ความพร้อมของหน่วยงาน	20

15. ประเด็นความเสี่ยงของโครงการและแนวทางการแก้ไข 21
16 กฎหมายที่เกี่ยวข้อง 21
17. ประโยชน์ที่จะได้รับ 21
ค. การลงนามรับรองโครงการ **22**
เอกสารอ้างอิง รายละเอียดคุณลักษณะเฉพาะ (Specification) **ภาคผนวก ก**
เอกสารอ้างอิง ใบเสนอราคา **ภาคผนวก ข**
เอกสารอ้างอิง แบบรายงานสรุปโครงการเพื่อพิจารณาความเหมาสมของ คุณลักษณะเฉพาะราคา (แบบ คกก.มท. ๐๑) และ ข้อมูลจากเว็บไซต์ **ภาคผนวก ค**

ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์ของรัฐที่มีมูลค่าเกินกว่า 100 ล้านบาทขึ้นไป

ก. ข้อมูลทั่วไป (หมายถึงข้อมูลทั่วไปของโครงการ เพื่อให้ทราบถึงข้อมูลในภาพรวม) อันประกอบไปด้วย

1.ชื่อโครงการ โครงการเช่าระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC)

2. ส่วนราชการ

2.1 ชื่อหน่วยงาน สำนักบริหารการทะเบียน กรมการปกครอง กระทรวงมหาดไทย

2.2 หัวหน้าส่วนราชการ **นายธนาคม จงจิระ** อธิบดีกรมการปกครอง

2.3 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) **นายสมยศ พุ่มน้อย** รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ

2.4 ผู้รับผิดชอบโครงการ **นางสาวลักษณา อภิรติปัญญา** ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

3. วงเงินงบประมาณทั้งโครงการจำนวน **948,359,900.00** บาท

โดยวงเงินผูกพัน 6 ปี งบประมาณ (72 งวด) แบ่งแยกการเบิกจ่าย ดังนี้

งบประมาณประจำปี	จำนวนเงิน (บาท)	ประเภทงบประมาณ
2566	58,482,190.00	งบประมาณแผ่นดิน
2567	139,092,780.00	งบประมาณแผ่นดิน
2568	158,059,980.00	งบประมาณแผ่นดิน
2569	158,059,980.00	งบประมาณแผ่นดิน
2570	158,059,980.00	งบประมาณแผ่นดิน
2571	158,059,980.00	งบประมาณแผ่นดิน
2572	118,545,010.00	งบประมาณแผ่นดิน

4. สัดส่วนของงบประมาณ (คิดเป็นร้อยละ) ระบุเงินงบประมาณที่ใช้ในแต่ละด้าน และคำนวณร้อยละของงบประมาณที่ใช้

สัดส่วน	ฮาร์ดแวร์	ซอฟต์แวร์	บำรุงรักษา	ดอกเบี้ย	อื่น ๆ	รวม
ด้าน IT						
ปี 2566	259,367,000.00 27.35%	122,307,816.37 12.90%	489,981,950.00 51.67%	54,404,554.69 5.74%	22,300,000.00 2.35%	948,361,321.06 100.00%
รวม IT	259,367,000.00 27.35%	122,307,816.37 12.90%	489,981,950.00 51.67%	54,404,554.69 5.74%	22,300,000.00 2.35%	948,361,321.06 100.00%
ด้าน Non-IT						
ปี 2566	-	-	-	-	-	-
รวม Non-IT	-	-	-	-	-	-
รวมทั้งหมด	**259,367,000.00 27.35%**	**122,307,816.37 12.90%**	**489,981,950.00 51.67%**	**54,404,554.69 5.74%**	**22,300,000.00 2.35%**	**948,361,321.06 100.00%**

หมายเหตุ ขอรับจัดสรรคงบประมาณ **948,359,900.00** บาท

5. การพิจารณาของคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ของกระทรวง

✓ ผ่านการพิจารณา ครั้งที่ .....

6. ความสอดคล้องกับยุทธศาสตร์ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

☐ ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

☐ ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

☐ ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล

☐ ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

☐ ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

✓ ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

ข. ข้อมูลโครงการ

1. หลักการและเหตุผลความเป็นมา

1.1 สำนักบริหารการทะเบียน กรมการปกครอง เป็นหน่วยงานหลักของประเทศที่มีระบบคอมพิวเตอร์แม่ข่ายที่ให้บริการงานประชาชน และบริการภาครัฐ ตลอดเวลา 7 วัน 24 ชั่วโมง โดยมีการดำเนินการพัฒนาระบบฐานข้อมูลของประเทศมาอย่างต่อเนื่อง และได้ปฏิรูปการบริหารจัดการภาครัฐ เพื่อการขับเคลื่อนและบริหารประเทศให้สามารถบริหารจัดการได้อย่างมีประสิทธิภาพ ตามโครงการการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ ทำให้เกิดการใช้ประโยชน์ข้อมูลขนาดใหญ่ในการบริการประชาชน ซึ่งกรมการปกครองและหน่วยงานรัฐต่าง ๆ ได้พัฒนาการบริการประชาชนให้เป็นไปตามความต้องการเฉพาะตัวบุคคลมากขึ้น พัฒนาโปรแกรมออนไลน์เพื่อให้ประชาชนสามารถเข้าถึงบริการภาครัฐได้สะดวกรวดเร็วยิ่งขึ้น ทำให้มีข้อมูลต่าง ๆ ไหลเวียนอยู่บนโลกออนไลน์ ซึ่งการรักษาความปลอดภัยทางไซเบอร์จึงจำเป็นอย่างยิ่ง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.2 กรมการปกครอง กระทรวงมหาดไทย เป็นหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางด้านสารสนเทศของประเทศ ในด้านความมั่นคงของรัฐและด้านบริการภาครัฐ ที่สำคัญที่จะต้องปฏิบัติ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.3 ตามราชกิจจานุเบกษา ในปี 2559 ประกาศรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด โดยมีกรมการปกครองอยู่ในรายชื่อ CII (critical information infrastructure)

1.4 ตามประกาศพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดนโยบายให้จัดตั้งคณะทำงาน และจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. 2562 ถึงแม้กรมการปกครองจะเป็นหน่วยงานที่ได้รับการยกเว้น แต่ในประกาศมีเขียนระบุให้มีการป้องกันและรักษาความปลอดภัย ตามมาตรฐานที่กำหนด โดยให้ยึดตามประกาศของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563

2. วัตถุประสงค์

2.1 เพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของข้อมูลต่าง ๆ ที่อยู่บนโลกออนไลน์

2.2 เพื่อเพิ่มประสิทธิภาพให้กับโครงข่ายระบบสารสนเทศ ของสำนักบริหารการทะเบียน กรมการปกครอง ให้มีความเสถียรภาพมากขึ้น

2.3 เพื่อเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามทางไซเบอร์

3. เป้าหมาย

3.1 ติดตั้งอุปกรณ์ป้องกันรักษาความปลอดภัยระบบคอมพิวเตอร์ส่วนกลาง 2 แห่ง ประกอบด้วย สำนักบริหารการทะเบียน คลองเก้า อำเภอลำลูกกา จังหวัดปทุมธานี และ วังไชยา นางเลิ้ง กรุงเทพมหานคร

3.2 ติดตั้งซอฟต์แวร์ระบบเพื่อป้องกัน , ตรวจจับ และ บริหารจัดการคอมพิวเตอร์ส่วนกลางและภูมิภาคทั่วประเทศ

4. โครงการที่จัดหาครั้งนี้ เป็นการที่จัดหาใหม่หรือทดแทนระบบเดิม

จัดหาใหม่

5. สภาพปัจจุบัน

5.1 สถานภาพระบบคอมพิวเตอร์ปัจจุบัน (ให้อธิบายภาพรวมของระบบคอมพิวเตอร์ทั้งหมดที่มีในปัจจุบันว่ามีระบบอะไรบ้างพอสังเขป)

ระบบคอมพิวเตอร์ปัจจุบันที่ให้บริการประชาชนทั่วประเทศ ได้ดำเนินการเช่าระบบให้บริการประชาชนทางด้านการทะเบียนและบัตรประจำตัวประชาชน

- ตามสัญญาเช่าเลขที่ 73/2562 ลงวันที่ 2 พฤษภาคม พ.ศ. 2562 วงเงิน 3,415,000,000 บาท (สามพันสี่ร้อยสิบห้าล้านบาท) สัญญามีผลตั้งแต่เดือน ตุลาคม พ.ศ. 2562 และจะสิ้นสุดเดือนกันยายน พ.ศ. 2568 รวม 6 ปี ติดตั้งทั้งสำนักบริหารการทะเบียนส่วนกลาง ศูนย์บริหารการทะเบียนภาค สาขาจังหวัด และสำนักทะเบียน ดังนี้
  1. สำนักบริหารการทะเบียน กรมการปกครอง คลองเก้า อำเภอลำลูกกา จังหวัดปทุมธานี สำนักบริหารการทะเบียน วังไชยา นางเลิ้ง กรุงเทพ
  2. ศูนย์บริหารการทะเบียนภาค 9 แห่ง และศูนย์บริหารการทะเบียนภาคสาขาจังหวัดทุกแห่ง สำนักทะเบียนอำเภอ/ท้องถิ่น 1,028 แห่ง
- ตามสัญญาเช่าเลขที่ 95/2564 ลงวันที่ 13 กันยายน พ.ศ. 2564 รวมระยะเวลา 6 ปี วงเงิน 891,106,800 บาท (แปดร้อยเก้าสิบเอ็ดล้านหนึ่งแสนหกพันแปดร้อยบาท)

5.2 สภาพปัญหาของผู้รับบริการ ผู้เกี่ยวข้องที่มีส่วนได้ส่วนเสีย ตลอดจนผู้ประกอบการเอกชนหรือประชาชนโดยรวม (หมายถึงเหตุผลความจำเป็นที่จะต้องซื้อหาระบบคอมพิวเตอร์ว่าเกิดจากปัญหาใด แล้วผู้ได้รับผลกระทบหากมีการพัฒนาระบบนี้ขึ้น เช่น เพื่อให้บริการประชาชน)

เนื่องจากกรมการปกครองเป็นระบบการให้บริการพื้นฐานของประเทศ หากมีภัยคุกคามหรือถูกโจมตีจะทำระบบไม่สามารถให้บริการประชาชนได้ หรืออาจทำให้ฐานข้อมูลของประเทศได้รับความเสียหาย และจากการที่ประกาศพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงจำเป็นต้องจัดตั้งและเสริมสร้างและเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

5.3 ระบบหรืออุปกรณ์ที่มีอยู่ในปัจจุบันของหน่วยงาน (ให้ระบุรายการอุปกรณ์ของหน่วยงานที่มีอยู่ในปัจจุบัน สถานที่ติดตั้งของระบบ หน่วยงานที่รับผิดชอบ)

ลำดับที่	รายการอุปกรณ์	จำนวน	ปีที่จัดหา	สถานที่ติดตั้ง	หน่วยงานรับผิดชอบ
1	ระบบแม่ข่ายให้บริการ (Server System)	4 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
2	ระบบหน่วยความจำสำรอง (Storage System)	2 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
3	ระบบสำรองข้อมูล (Backup System)	2 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
4	ระบบจัดสรรงาน (Load Balancer)	4 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท

ลำดับที่	รายการอุปกรณ์	จำนวน	ปีที่จัดหา	สถานที่ติดตั้ง	หน่วยงานรับผิดชอบ
5	ตู้สำหรับติดตั้งเครื่องแม่ข่าย ชนิด Blade (Enclosure/Chassis)	8 ตู้	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
6	แผงวงจรเครื่องคอมพิวเตอร์แม่ข่าย ชนิด Blade สำหรับตู้ Enclosure/Chassis	108 หน่วย	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
7	ตู้สำหรับจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ แบบที่ 3 (ขนาด 42U)	4 ตู้	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
8	เครื่องคอมพิวเตอร์แม่ข่าย แบบที่ 2 (Domain Name Server)	8 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
9	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L3 Switch) จุดเชื่อมต่อแต่ละชั้นอาคาร	10 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
10	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L3 Switch) สำหรับแกนสื่อสารหลักของอาคาร	2 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
11	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L3 Switch) สำหรับใช้งาน Server Zone	4 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
12	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L2 Switch) ขนาด 24 ช่อง แบบที่ 2 สำหรับ Console Zone	4 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
13	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L2 Switch) ขนาด 24 ช่อง แบบที่ 2 สำหรับ Replicate Zone	2 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
14	อุปกรณ์ Internet Firewall	4 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
15	อุปกรณ์ Internet Proxy Gateway	1 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
16	ระบบบริหารจัดการพิสูจน์สิทธิ์เพื่อเข้าใช้งานในเครือข่าย (LDAP)	2 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
17	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L2 Switch) สำหรับใช้งาน DMZ Zone และ WAF Zone	8 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
18	ระบบปรับอากาศ สำหรับห้องคอมพิวเตอร์	7 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
19	ระบบเครื่องจ่ายไฟฟ้าสำรองส่วนกลาง (UPS)	3 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
20	ระบบสวิตช์เปลี่ยนแหล่งจ่ายไฟอัตโนมัติ (ATS)	2 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
21	ระบบสัญญาณเตือนภัย (Fire Alarm)	2 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
22	เครื่องฉายภาพดิจิตอล (Projector)	10 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
23	เครื่องคอมพิวเตอร์โน้ตบุ๊ก สำหรับงานประมวลผล	890 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
24	เครื่องคอมพิวเตอร์ สำหรับงานประมวลผล แบบที่ 1	6,559 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา สำนักทะเบียน	สน.บท

ลำดับที่	รายการอุปกรณ์	จำนวน	ปีที่จัดหา	สถานที่ติดตั้ง	หน่วยงานรับผิดชอบ
25	เครื่องคอมพิวเตอร์ สำหรับงานประมวลผล แบบที่ 2	30 เครื่อง	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
26	อุปกรณ์อ่านลายพิมพ์นิ้วมือ (Thumb Scanner)	1,182 เครื่อง	2562	สำนักทะเบียน	สน.บท
27	อุปกรณ์สำรองไฟฟ้า (UPS)	2,176 เครื่อง	2562	สำนักทะเบียน	สน.บท
28	อุปกรณ์ป้องกันไฟฟ้ากระชาก (Surge Protection)	573 ชุด	2562	สำนักทะเบียน	สน.บท
29	กล้องถ่ายภาพ DSLR	1,021 เครื่อง	2562	สำนักทะเบียน	สน.บท
30	ขาตั้งกล้อง (Camera Stand)	1,021 ชุด	2562	สำนักทะเบียน	สน.บท
31	อุปกรณ์แปลงไฟฟ้ากล้องถ่ายภาพ DSLR (AC Power Adapter)	1,021 ชุด	2562	สำนักทะเบียน	สน.บท
32	ระบบคิวพร้อมอุปกรณ์	100 ชุด	2562	สำนักทะเบียน	สน.บท
33	เครื่องปรับอากาศสำนักทะเบียน	573 เครื่อง	2562	สำนักทะเบียน	สน.บท
34	อุปกรณ์กระจายสัญญาณไร้สาย (Access Point)	156 เครื่อง	2562	สำนักทะเบียน	สน.บท
35	อุปกรณ์อ่านเขียนบัตรสมาร์ทการ์ด (Smart Card Reader)	7,591 เครื่อง	2562	สำนักทะเบียน	สน.บท
36	เครื่องพิมพ์ชนิดเลเซอร์ หรือชนิด LED ขาวดำ ชนิด Network แบบที่ 1	5,360 เครื่อง	2562	สำนักทะเบียน	สน.บท
37	อุปกรณ์กระจายสัญญาณสื่อสารข้อมูล (L2 Switch) ขนาด 24 ช่อง แบบที่ 2	1,593 เครื่อง	2562	สำนักทะเบียน	สน.บท
38	เครื่องพิมพ์ความเร็วสูง (Line Printer)	740 เครื่อง	2562	สำนักทะเบียน	สน.บท
39	เครื่องพิมพ์สมุดทะเบียนบ้าน (Passbook Printer)	1,828 เครื่อง	2562	สำนักทะเบียน	สน.บท
40	เครื่องพิมพ์บัตรประจำตัวประชาชน (ID Card Printer)	1,202 เครื่อง	2562	สำนักทะเบียน	สน.บท
41	อุปกรณ์อ่านเขียนบัตรประจำตัวประชาชน พร้อมอ่านและจัดเก็บรหัสลายนิ้วมือลง CHIP	1,262 เครื่อง	2562	สำนักทะเบียน	สน.บท
42	ชุดโปรแกรมระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์โน้ตบุ๊ก	7,379 ชุด	2562	สน.บท ลำลูกกา/วังไชยา, สำนักทะเบียน	สน.บท
43	ลิขสิทธิ์การใช้ซอฟต์แวร์ระบบจัดการฐานข้อมูลเครื่องแม่ข่ายให้บริการด้านฐานข้อมูล	2 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
44	ลิขสิทธิ์การใช้ซอฟต์แวร์ระบบการจัดการขั้นตอนการทำงานโปรแกรมประยุกต์	1 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
45	ลิขสิทธิ์การใช้ซอฟต์แวร์เปรียบเทียบลักษณะลายพิมพ์นิ้วมือ	1 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
46	ลิขสิทธิ์การใช้ซอฟต์แวร์เปรียบเทียบลักษณะภาพใบหน้า	1 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา	สน.บท
47	ระบบโปรแกรมประยุกต์การให้บริการงานทะเบียนราษฎรและบัตรประจำตัวประชาชน	1 ระบบ	2562	สน.บท ลำลูกกา/วังไชยา สำนักทะเบียน	สน.บท
48	ระบบคอมพิวเตอร์สำหรับ Virtualization Machine System	2 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท

ลำดับที่	รายการอุปกรณ์	จำนวน	ปีที่จัดหา	สถานที่ติดตั้ง	หน่วยงานรับผิดชอบ
49	ระบบจัดการสำรองข้อมูลแบบรวมศูนย์ (Offsite Backup)	1 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
50	ระบบหน่วยความจำสำรองสำหรับจัดเก็บข้อมูลภาพ (Image Storage System)	2 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
51	เครื่องสำรองไฟฟ้าห้องเครื่องแม่ข่ายคอมพิวเตอร์	2 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
52	ระบบเครื่องปรับอากาศสำหรับเครื่องจ่ายไฟฟ้าสำรอง	4 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
53	อุปกรณ์กระจายสัญญาณ (L3 Switch) 25 Gbps ขนาด 48 ช่อง	4 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
54	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10 Gbps ขนาด 48 ช่อง	4 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
55	อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)	4 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
56	อุปกรณ์กระจายสัญญาณ (L2 Switch) 1 Gbps ขนาด 24 ช่อง	8 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
57	อุปกรณ์ Internet Proxy Gateway	1 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
58	ระบบตรวจสอบรายชื่อผู้ใช้งาน (Radius System)	2 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
59	อุปกรณ์ควบคุมการทำงานของระบบไร้สาย (Wireless Controller)	4 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
60	อุปกรณ์กระจายสัญญาณของระบบไร้สาย (Wireless Access Point)	135 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
61	อุปกรณ์กระจายสัญญาณ (L2 PoE Switch) ขนาด 24 ช่อง	10 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
62	ระบบรักษาความปลอดภัย Access Control และระบบกล้อง CCTV ควบคุมการเปิด/ปิด ประตูห้องเครื่องแม่ข่ายคอมพิวเตอร์	2 ระบบ	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
63	กล้องโทรทัศน์วงจรปิดชนิดเครือข่าย แบบมุมมองคงที่สำหรับติดตั้งภายในอาคารสำหรับใช้ในงานรักษาความปลอดภัยทั่วไป	14 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
64	กล้องโทรทัศน์วงจรปิดชนิดเครือข่าย แบบปรับมุมมอง แบบที่1 สำหรับใช้ในงานรักษาความปลอดภัยทั่วไป	4 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
65	อุปกรณ์บันทึกภาพผ่านเครือข่าย (Network Vidow Recorder)	2 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
66	อุปกรณ์กระจายสัญญาณแบบ PoE (PoE L2 Switch) ขนาด 16 ช่อง	2 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
67	อุปกรณ์ Access Control	12 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
68	ซอฟต์แวร์บริหารจัดการ Access Control	2 ชุด	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท
69	อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง แบบที่ 2	2 หน่วย	2564	สน.บท ลำลูกกา/วังไชยา	สน.บท

ลำดับที่	รายการอุปกรณ์	จำนวน	ปีที่จัดหา	สถานที่ติดตั้ง	หน่วยงานรับผิดชอบ
70	คอมพิวเตอร์ สำหรับงานประมวลผล แบบที่ 1	4,013 หน่วย	2564	สำนักทะเบียน	สน.บท
71	อุปกรณ์กระจายสัญญาณ (L2 Switch) ขนาด 24 ช่อง แบบที่ 2	719 หน่วย	2564	สำนักทะเบียน	สน.บท
72	สแกนเนอร์ สำหรับงานเก็บเอกสารทั่วไป	7,529 หน่วย	2564	สำนักทะเบียน	สน.บท
73	เครื่องพิมพ์เลเซอร์ หรือ LED ขาดดำ ชนิด Network แบบที่ 1	3,526 หน่วย	2564	สำนักทะเบียน	สน.บท
74	เครื่องพิมพ์สมุดทะเบียนบ้าน (Passbook Printer)	1,410 หน่วย	2564	สำนักทะเบียน	สน.บท
75	เครื่องพิมพ์ความเร็วสูง (Line Pritner)	294 หน่วย	2564	สำนักทะเบียน	สน.บท
76	เครื่องสำรองไฟฟ้า ขนาด 3kVA	1,208 หน่วย	2564	สำนักทะเบียน	สน.บท
77	เครื่องอ่านบัตรแบบอเนกประสงค์ (Smart Card Reader)	10,668 หน่วย	2564	สำนักทะเบียน	สน.บท
78	เครื่องอ่านเขียนบัตรสมาร์ทการ์ด พร้อมจัดเก็บลายพิมพ์นิ้วมือลง Chip	5 หน่วย	2564	สำนักทะเบียน	สน.บท
79	กล้องถ่ายภาพ ระบบบัตรประจำตัวประชาชน	166 หน่วย	2564	สำนักทะเบียน	สน.บท
80	อุปกรณ์แปลงสัญญาณไฟฟ้ากล้องถ่ายภาพ DSLR (AC Power Adapter)	166 หน่วย	2564	สำนักทะเบียน	สน.บท
81	ขาตั้งกล้อง	166 หน่วย	2564	สำนักทะเบียน	สน.บท
82	เครื่องปรับอากาศ ชนิดตั้งพื้นหรือชนิดแขวน ขนาด 18,000 บีทียู	663 หน่วย	2564	สำนักทะเบียน	สน.บท
83	ระบบคิวและระบบประชาสัมพันธ์	84 หน่วย	2564	สำนักทะเบียน	สน.บท
84	ชุดโปรแกรมระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์โน๊ตบุ๊ค แบบสิทธิการใช้งาน ประเภทติดตั้งมาจากโรงงาน (OEM) ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย	4,019 หน่วย	2564	สำนักทะเบียน	สน.บท
85	อุปกรณ์ป้องกันไฟฟ้ากระชาก (Surge Protection)	455 หน่วย	2564	สำนักทะเบียน	สน.บท
86	เครื่องคอมพิวเตอร์โน๊ตบุ๊ค สำหรับงานประมวลผล	6 หน่วย	2564	สำนักทะเบียน	สน.บท
87	เครื่องพิมพ์บัตรประจำตัวประชาชน (IDCard Printer)	5 หน่วย	2564	สำนักทะเบียน	สน.บท
88	อุปกรณ์อ่านลายพิมพ์นิ้วมือ	5 หน่วย	2564	สำนักทะเบียน	สน.บท
89	โต๊ะวางเครื่องคอมพิวเตอร์พร้อมเก้าอี้	177 หน่วย	2564	สำนักทะเบียน	สน.บท
90	ฉากประกอบการถ่ายรูปแบบเคลื่อนที่	5 หน่วย	2564	สำนักทะเบียน	สน.บท

6. ระบบงานและปริมาณงานที่จะดำเนินการ

6.1 ความแตกต่างของระบบเดิมกับระบบใหม่ (หากมีเป็นระบบที่จัดหาใหม่เพื่อทดแทนระบบเดิมให้อธิบายพอสังเขป)

6.1.1 จัดทำศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) สำหรับกรมการปกครอง กระทรวงมหาดไทย 1 แห่ง ณ สำนักบริหารการทะเบียน คลองเก้า อำเภอลำลูกกา จังหวัดปทุมธานี

6.1.2 ติดตั้งซอฟต์แวร์ในคอมพิวเตอร์ส่วนภูมิภาค ทั่วประเทศ

- ติดตั้งซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software)
- ติดตั้งระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response)

6.2 ลักษณะและปริมาณงาน (ปริมาณข้อมูล ความถี่ในการเรียกใช้ข้อมูลกลุ่มผู้ใช้งาน จำนวนผู้ใช้งานทั้งหมด และจำนวนผู้ใช้งานสูงสุดในเวลาเดียวกัน)

ข้อมูลโดยประมาณ	ประชากร	ทะเบียนราษฎร (รายการ)	บัตรประจำตัวประชาชน (รายการ)	ทะเบียนทั่วไป (รายการ)
ประจำปี 2554	64.07 ล้านคน	17.4 ล้าน	12.5 ล้าน	2.9 ล้าน
ประจำปี 2555	64.45 ล้านคน	17.3 ล้าน	10.3 ล้าน	2.8 ล้าน
ประจำปี 2556	64.79 ล้านคน	20.5 ล้าน	10.1 ล้าน	3.0 ล้าน
ประจำปี 2557	65.12 ล้านคน	21.1 ล้าน	9.7 ล้าน	3.1 ล้าน
ประจำปี 2558	65.73 ล้านคน	22.1 ล้าน	12.1 ล้าน	3.1 ล้าน
ประจำปี 2559	65.93 ล้านคน	20.5 ล้าน	12.8 ล้าน	2.9 ล้าน
ประจำปี 2560	66.19 ล้านคน	20.3 ล้าน	10.2 ล้าน	2.8 ล้าน
ประจำปี 2561	66.41 ล้านคน	20.1 ล้าน	8.4 ล้าน	2.9 ล้าน
ประจำปี 2562	66.56 ล้านคน	20.2 ล้าน	7.4 ล้าน	2.9 ล้าน
ประจำปี 2563	66.19 ล้านคน	22.0 ล้าน	7.9 ล้าน	2.9 ล้าน

ปริมาณงานการให้บริการข้อมูลแก่หน่วยงานภายนอกสำนักบริหารการทะเบียนตามข้อตกลงการใช้ประโยชน์จากฐานข้อมูลกลาง (MOU)

ข้อมูลโดยประมาณ	จำนวนปริมาณงาน (รายการ)
ประจำปี 2553	144,856,672
ประจำปี 2554	107,587,391
ประจำปี 2555	93,763,751
ประจำปี 2556	158,318,841
ประจำปี 2557	144,379,890
ประจำปี 2558	301,556,292
ประจำปี 2559	398,519,430
ประจำปี 2560	294,113,322
ประจำปี 2561	445,323,715
ประจำปี 2562	609,213,754
ประจำปี 2563	267,007,782

6.3 ระบบงานและวิธีการนำเข้าข้อมูล (หากในระบบจะต้องมีการนำเข้าข้อมูลเดิม มีแผนในการจัดการนำเข้าอย่างไร หรือจัดการกับข้อมูลเดิมที่มีอยู่อย่างไร)

- ไม่มี

7. สถาปัตยกรรมการจัดการองค์กร (Enterprise Architecture) ซึ่งมีองค์ประกอบดังนี้

7.1 สถาปัตยกรรมการจัดการองค์กรด้านพันธกิจ (Business Architecture) ควรประกอบไปด้วย

7.1.1 ความสอดคล้องเชิงยุทธศาสตร์ของโครงการ (เช่น นโยบายรัฐบาล, แผนแม่บท ICT, แผนยุทธศาตร์ เป็นต้น)

7.1.1.1 นโยบายรัฐบาล

- การบริหารกิจการบ้านเมืองที่ดี (Good Governance)
- การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์ (E-Government) แผนการบริหารราชการแผ่นดิน
- ประสิทธิภาพการบริหารราชการแผ่นดิน การบริหารงานภาครัฐมีประสิทธิภาพ มีคุณภาพและมีธรรมาภิบาล ได้รับความเชื่อมั่นศรัทธาจากประชาชน บุคลากรภาครัฐมีขีดความสามารถสูงขึ้นมีคุณธรรม จริยธรรม สามารถปฏิบัติงานได้อย่างมืออาชีพ ได้รับความเป็นธรรมในการปฏิบัติราชการ

7.1.1.2 แผนการบริหารราชการแผ่นดิน

- ประสิทธิภาพการบริหารราชการแผ่นดิน การบริหารงานภาครัฐมีประสิทธิภาพ มีคุณภาพ และมีคุณภาพ และมีธรรมาภิบาล ได้รับความเชื่อมั่นศรัทธาจากประชาชน บุคลากรภาครัฐมีขีดความสามารถสูงขึ้น มีคุณธรรม จริยธรรม สามารถปฏิบัติงาน ได้อย่างมืออาชีพ ได้รับความเป็นธรรมในการปฏิบัติราชการ

7.1.1.3 แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

- ประเด็นยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล เป็นการมุ่งใช้เทคโนโลยีดิจิทัลในการปรับปรุงประสิทธิภาพการบริหารจัดการของหน่วยงานรัฐทั้งส่วนกลางและส่วนภูมิภาค ให้เกิดบริการภาครัฐในรูปแบบดิจิทัลที่ประชาชนเข้าถึงบริการได้โดยไม่มีข้อจำกัดทางกายภาพ พื้นที่ และภาษา นำไปสู่การหลอมรวมการทำงานภาครัฐเสมือนเป็นองค์กรเดียว

7.1.1.4 แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560-2564)

- ยุทธศาสตร์ที่ 6 การบริหารจัดการในภาครัฐ การป้องกันการทุจริตประพฤติมิชอบและธรรมา ภิบาลในสังคมไทย ข้อ 2 เพิ่มประสิทธิภาพและยกระดับการให้บริการสาธารณะให้ได้มาตรฐานสากล - ปรับรูปแบบการให้บริการของรัฐจากรูปแบบเดิมไปสู่การให้บริการประชาชนผ่านระบบดิจิทัลอย่างเป็นระบบ ลดขั้นตอนการดำเนินงาน ให้สอดคล้องกับวิถีการดำเนินชีวิตและความต้องการของผู้รับบริการแต่ละบุคคล

7.1.1.5 แผนยุทธศาสตร์กระทรวงมหาดไทย พ.ศ 2560-2564

- ประเด็นยุทธศาสตร์ที่ 3 การเสริมสร้างความสงบเรียบร้อยและความมั่นคงภายใน เป้าประสงค์ ข้อ 3.3 ระบบข้อมูลมีความถูกต้อง เชื่อถือได้ และถูกนำไปใช้ในการพัฒนาประเทศ กลยุทธ์ ข้อ 3.3.1 ส่งเสริมการนำเทคโนโลยีดิจิทัลไปใช้ในการปรับปรุงระบบข้อมูลบุคคลและข้อมูลในการพัฒนา กลยุทธ์ ข้อ 3.3.2 พัฒนาระบบฐานข้อมูลกลาง (One Info)

โดยเชื่อมโยง ข้อมูลระหว่างหน่วยงานผ่านระบบอิเล็กทรอนิกส์/เทคโนโลยีดิจิทัล เพื่อนำไปใช้ในการพัฒนาประเทศ

- ประเด็นยุทธศาสตร์ที่ 4 การวางรากฐานการพัฒนาองค์กรอย่างสมดุล เป้าประสงค์ ข้อ 4.1 องค์กรมีการบริหารจัดการที่ดีและองค์กรปกครองส่วนท้องถิ่น มีความเข้มแข็ง กลยุทธ์ ข้อ 4.1.2 เพิ่มประสิทธิภาพการปฏิบัติงานและการให้บริการประชาชนในรูปแบบดิจิทัล (Digital Service) และบริการเบ็ดเสร็จ (One Stop Service) กลยุทธ์ ข้อ 4.1.3 เพิ่มช่องทางการเข้าถึงบริการภาครัฐ

7.1.1.6 แผนยุทธศาสตร์กรมการปกครอง พ.ศ 2560-2564

- ประเด็นยุทธศาสตร์ที่ 4 การพัฒนาระบบบริการและข้อมูลบุคคลให้ทันสมัยมีคุณภาพเพื่อความมั่นคงและการพัฒนาประเทศ กลยุทธ์ข้อ 4.1.1 จัดทำ เชื่อมโยงและพัฒนาระบบฐานข้อมูลทะเบียนบุคคล และระบบการรักษาความปลอดภัยที่มีมาตรฐาน กลยุทธ์ ข้อ 4.1.2 พัฒนาและส่งเสริมการใช้บัตรประชาชนแบบ Smart Card ในการรับบริการเพียงใบเดียวแบบเบ็ดเสร็จ กลยุทธ์ ข้อ 4.1.3 สร้าง Application หรือนวัตกรรมงานทะเบียนและงานบริการอื่นๆ ให้ประชาชนสามารถเข้าถึงการบริการได้สะดวก รวดเร็ว แบบจุดเดียวเบ็ดเสร็จ (One Stop Service)

7.1.2 คำจำกัดความของระบบอย่างย่อ

ระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) ศูนย์ปฏิบัติการที่มีทีมทำหน้าที่เฝ้าระวังภัยคุกคามขององค์กร ทำหน้าที่ตรวจสอบการเข้าถึงเครือข่ายและระบบสารสนเทศต่าง ๆ ขององค์กรตลอดเวลาแบบ 24/7 หากพบพฤติกรรมที่ผิดปกติ เช่น พบการละเมิดข้อมูลสำคัญ ๆ หรือการโจมตีทางไซเบอร์ขององค์กร ก็พร้อมตอบสนองต่อเหตุการณ์อย่างรวดเร็วและสามารถหยุดการโจมตี รวมทั้งเก็บข้อมูลเพื่อตรวจหาช่องทางที่อาชญากรบุกรุกเข้ามาได้อย่างแม่นยำ สำหรับวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคาม และ/หรือเหตุการณ์ผิดปกติอันอาจก่อให้เกิดความเสียหายอย่างรุนแรงกับข้อมูลและระบบสารสนเทศของระบบฐานข้อมูลของประเทศให้เป็นไปอย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานสากลและสามารถรับมือภัยคุกคามที่เกิดขึ้นในโลกไซเบอร์ได้

7.1.3 กระบวนการดำเนินงาน

จัดหาอุปกรณ์เพื่อจัดตั้งศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) สำหรับกรมการปกครอง กระทรวงมหาดไทย

7.1.4 ผู้ใช้งานระบบ

หน่วยงานภายใต้กรมการปกครอง กระทรวงมหาดไทย

7.1.5 กฎหมายข้อบังคับที่เป็นอุปสรรค

- ไม่มี

7.2 สถาปัตยกรรมการจัดการองค์กรด้านระบบสารสนเทศ (Application Architecture) ควรประกอบไปด้วย

7.2.1 ชื่อของระบบสารสนเทศ

- ไม่มี

7.2.2 High level application flow with user roles participationing (SOD)

- ไม่มี

7.2.3 โปรแกรมประยุกต์อื่นๆที่ต้องเชื่อมโยงด้วย (รวมถึงชื่อของหน่วยงานเจ้าของระบบ)

- ไม่มี

7.3 สถาปัตยกรรมการจัดการองค์กรด้านข้อมูล (Data Architecture) ควรประกอบไปด้วย

7.3.1 ข้อมูลที่จำเป็นของระบบ

- ไม่มี

7.3.2 ชื่อของหน่วยงานเจ้าของข้อมูล

- ไม่มี

7.3.3 โครงสร้างฐานข้อมูล

- ไม่มี

7.3.4 ข้อมูลนั้นมี change control หรือไม่

- ไม่มี

7.3.5 มาตรฐานการแลกเปลี่ยนข้อมูลที่ใช้ เช่น TH e-GIF, StatXML, ebXML เป็นต้น

- ไม่มี

7.4 สถาปัตยกรรมการจัดการองค์กรด้านเทคโนโลยี (Technology Architecture) ควรประกอบไปด้วย

7.4.1 ภาษาที่ใช้ในการพัฒนาระบบสารสนเทศ

- ไม่มี

7.4.2 ระบบปฏิบัติการของระบบสารสนเทศ

- ไม่มี

7.4.3 ค่าใช้จ่ายในการบำรุงรักษาระบบสารสนเทศต่อปี

- ใช้อัตราค่าบำรุงรักษาเฉลี่ย 10% ต่อปี

7.4.4 ระบบปฏิบัติการของระบบฐานข้อมูล

- ไม่มี

7.4.5 อัตราการเพิ่มของข้อมูล (%)

- 15 % ต่อปี

7.4.6 ค่าใช้จ่ายในการบำรุงรักษาระบบฐานข้อมูลต่อปี

- ไม่มี

7.4.7 การวิเคราะห์ปัญหาของระบบงานเดิม และทางเลือกในการออกแบบระบบ

ปัจจุบันกรมการปกครอง กระทรวงมหาดไทย ไม่มีศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center: SOC) และเพื่อให้เป็นไปตามประกาศพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงจำเป็นต้องจัดตั้งและเสริมสร้างความรู้และศักยภาพ

ของผู้ปฏิบัติงานหรือผู้ที่เกี่ยวข้องกับการเฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศได้เรียนรู้และฝึกปฏิบัติอย่างเข้มข้นในการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ การจัดทำรายงานต่างๆ จากการเฝ้าระวัง การวิเคราะห์ข้อมูลล็อกโดยใช้ซอฟต์แวร์เชิงพาณิชย์ และการจัดเก็บหลักฐานเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อตรวจสอบช่องทางการเข้าถึงเครือข่ายและระบบสารสนเทศต่างๆ ที่ผิดปกติ เพื่อตอบสนองต่อเหตุการณ์และแก้ปัญหาการบุกรุกระบบอย่างรวดเร็วและมีประสิทธิภาพ

7.4.8 การวิเคราะห์ขนาดความสามารถทางความเร็วของซีพียู ขนาดหน่วยความจำ ความจุข้อมูลของดิสก์ และความเร็วในการสื่อสารข้อมูล ที่ต้องการตามปริมาณงานในข้อ 6

- คิดจากการวิเคราะห์ข้อมูล log ปริมาณ 30Gb ต่อวัน ที่จะต้องนำมาวิเคราะห์ในแต่ละวัน

7.4.9 ปัจจัยสำเร็จของโครงการ

7.4.9.1 ได้รับการสนับสนุน งบประมาณ

7.4.9.2 สามารถติดตั้งระบบได้อย่างครบถ้วน สมบูรณ์ ไม่เกิดปัญหา

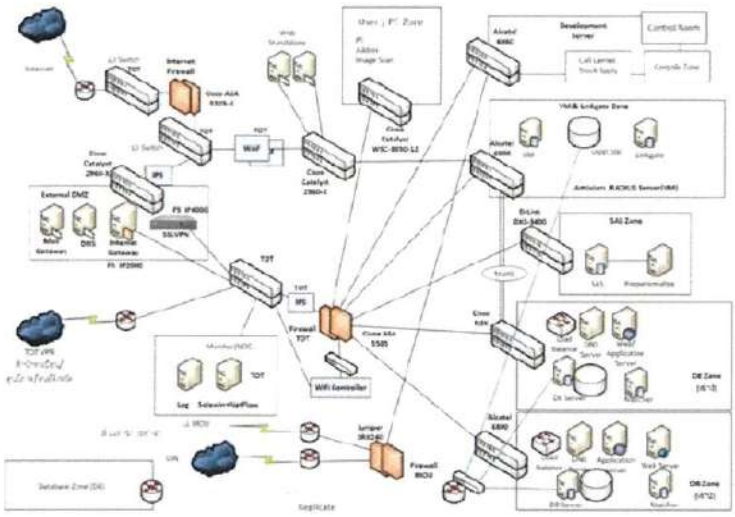
7.4.10 เทคโนโลยีของระบบที่เสนอ พร้อมเหตุผล

ตาม NIST Cyber Security Framework ประกอบด้วย

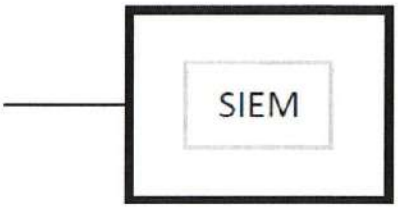
The National Institute of Standards and Technology (NIST)

NIST Cyber Security Framework		รายการที่จัดหา
Identify	การระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง	ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment)
		ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network)
		ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร
		อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย Network access control (NAC)
		ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง
		ระบบป้องกันภัยคุกคามโดยกลยุทธ์ (Deception Solution)
Protect	การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร	ระบบบริหารจัดการทรัพยากรบนเครือข่าย (Active Directory)
		อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)
		ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR)
		อุปกรณ์วิเคราะห์ความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)
		อุปกรณ์บริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)
		อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร
		ระบบป้องกันภัยคุกคาม Domain Name System
		อุปกรณ์ป้องกันเครือข่าย Internet Firewall
Detect	การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ	ระบบจัดเก็บข้อมูลและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)
		อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง
		อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์
Respond	การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูล ระบบเครือข่าย
		ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone
Recovery	การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม	ห้องปฏิบัติการ Security Operations Center (SOC)
		SOC TIER 1 Services Operator 24x7

7.4.11 แผนผังการเชื่อมโยงเครือข่าย (Network diagram)

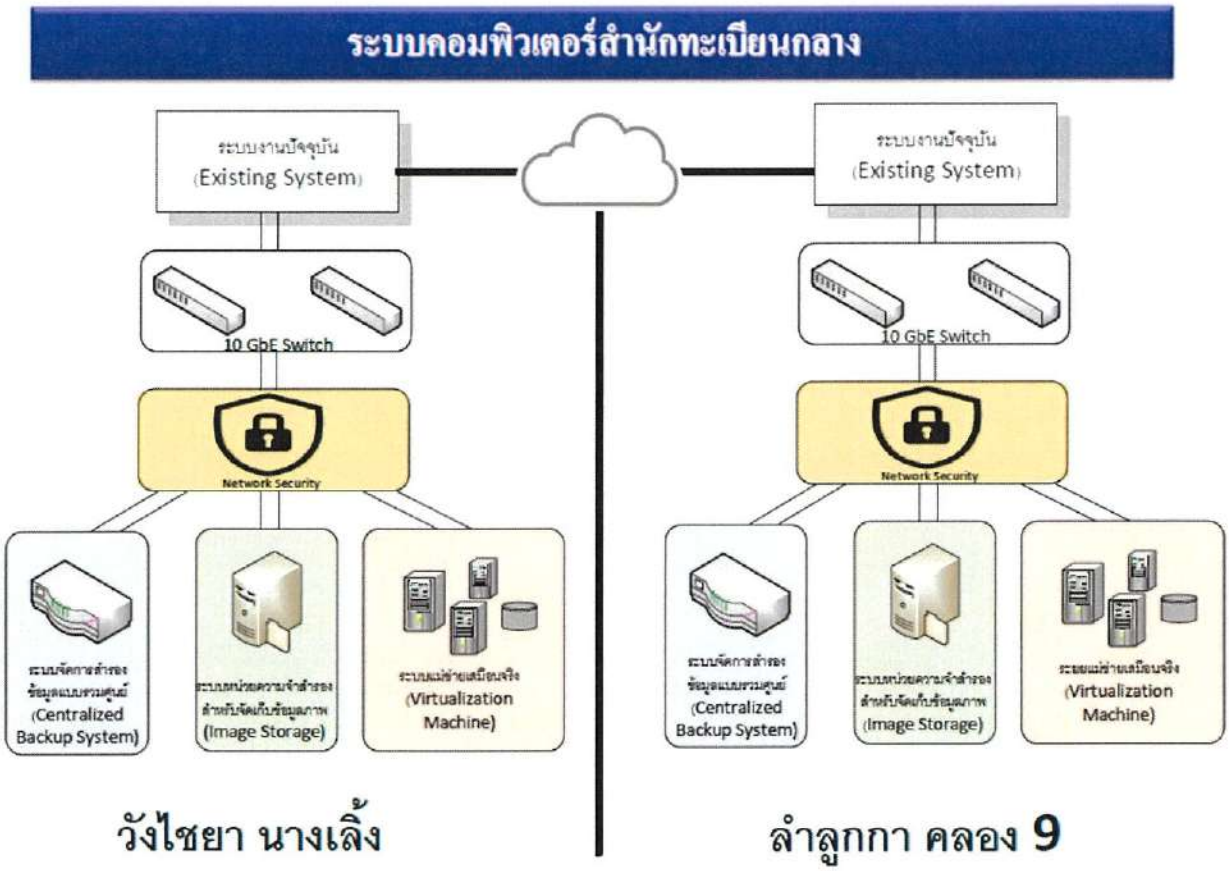


Existing Network



SOC

7.4.12 แผนผังการเชื่อมโยงระบบ (system diagram)



7.4.13 การรักษาความมั่นคงปลอดภัยสารสนเทศ (Network, System, and Information security)

7.4.13.1 มีอุปกรณ์รักษาความปลอดภัยเครือข่าย ประกอบด้วย Firewall แบ่งระบบออกเป็น zone ต่างๆ กำหนดค่า Policy ของการการเข้าถึงระบบต่างๆตามความจำเป็นเท่านั้น มี Proxy Gateway ที่มีระบบตรวจจับ threat/attack ต่างๆ จากการใช้งานเว็บไซต์ภายนอก มีระบบตรวจสอบรายชื่อของผู้ใช้งาน

7.4.13.2 จัดทำการระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง

7.4.13.3 มีการวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร

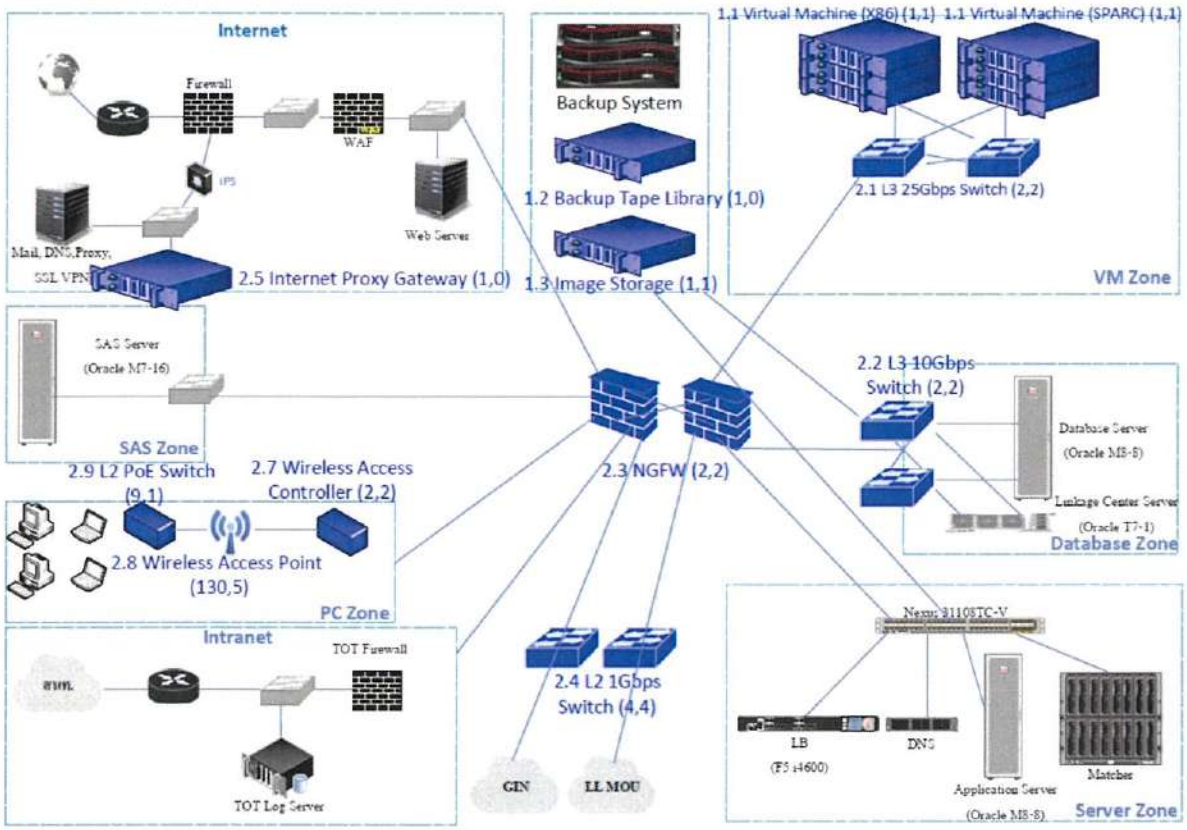
7.4.13.4 มีการกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ

7.4.13.5 มีการกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

7.4.13.6 มีการกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

7.4.13.7 เพิ่มการป้องกันการโจมตีจากภายในและภายนอกโครงข่ายสื่อสารข้อมูล

7.4.13.8 Network Diagram



8. รายการที่จะจัดหา

8.1 ค่าใช้จ่ายฮาร์ดแวร์ / ซอฟต์แวร์

ลำดับ	รายละเอียด	จำนวน	หน่วยนับ	ราคาต่อหน่วย	ราคารวมค่าเช่า 6 ปี	ที่มาของราคากลาง
ด้าน IT						
1. ฮาร์ดแวร์						
1.1	อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network access control)	2	เครื่อง	1,500,000.00	6,404,019.40	สืบราคาจากท้องตลาด
1.2	อุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution)	2	เครื่อง	15,587,200.00	50,959,954.16	สืบราคาจากท้องตลาด
1.3	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	4	เครื่อง	5,599,600.00	70,211,662.73	สืบราคาจากท้องตลาด
1.4	อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)	2	เครื่อง	1,195,300.00	7,493,749.59	สืบราคาจากท้องตลาด
1.5	อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection)	4	ระบบ	5,981,725.00	51,076,110.62	สืบราคาจากท้องตลาด
1.6	อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง	1	เครื่อง	9,700,000.00	15,856,329.40	สืบราคาจากท้องตลาด
1.7	อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์	1	เครื่อง	15,796,000.00	33,719,296.83	สืบราคาจากท้องตลาด
1.8	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย	1	เครื่อง	5,679,900.00	14,964,679.94	สืบราคาจากท้องตลาด
1.9	ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone	2	ระบบ	1,780,000.00	7,599,436.36	สืบราคาจากท้องตลาด
1.10	อุปกรณ์ป้องกันเครือข่าย Internet Firewall	4	เครื่อง	22,338,000.00	217,385,313.89	สืบราคาจากท้องตลาด
1.11	อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application ระหว่างศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า-นางเลิ้ง	4	เครื่อง	8,850,000.00	57,867,428.95	สืบราคาจากท้องตลาด
1.12	ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network)	2	ระบบ	2,196,400.00	8,978,392.14	สืบราคาจากท้องตลาด
1.13	อุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch	4	เครื่อง	1,994,000.00	13,038,152.92	สืบราคาจากท้องตลาด
1.14	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง	4	เครื่อง	1,155,000.00	7,552,189.88	สืบราคาจากท้องตลาด
รวมค่าฮาร์ดแวร์					**563,106,716.82**	

2. ซอฟต์แวร์						
2.1	ซอฟต์แวร์ระบบบริหารจัดการช่องโหว่ด้านความปลอดภัยระบบสารสนเทศ (Vulnerability Assessment)	1	ระบบ	1,372,000.00	4,643,771.54	สืบราคาจากท้องตลาด
2.2	ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor)	1	ระบบ	350,000.00	2,147,135.60	สืบราคาจากท้องตลาด
2.3	ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software)	11,500	หน่วย	850.00	50,191,429.89	สืบราคาจากท้องตลาด
2.4	ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response)	11,500	หน่วย	3,360.00	101,803,769.91	สืบราคาจากท้องตลาด
2.5	ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)	1	หน่วย	37,270,816.37	72,290,194.03	สืบราคาจากท้องตลาด
2.6	ระบบป้องกันภัยคุกคาม Domain Name System	500	หน่วย	3,800.00	11,655,878.96	สืบราคาจากท้องตลาด
2.7	ระบบจัดเก็บข้อมูลและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)	1	ระบบ	28,500,000.00	50,863,184.33	สืบราคาจากท้องตลาด
2.8	สิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) บนอุปกรณ์ Internet Proxy Gateway	1000	หน่วย	4,500.00	11,106,029.10	สืบราคาจากท้องตลาด
รวมค่าซอฟต์แวร์					304,701,393.35	
3. ค่าบุคลากร/ที่ปรึกษา						
รวมค่าบุคลากร/ที่ปรึกษา						
4. ค่าฝึกอบรม						
รวมค่าฝึกอบรม						
5. ค่าใช้จ่ายอื่น ๆ						
5.1	ห้องปฏิบัติการ Security Operations Center (SOC)	1	หน่วย	2,500,000.00	4,086,682.84	สืบราคาจากท้องตลาด
5.2	SOC Services Operators 24x7	12	หน่วย	900,000.00	66,254,469.85	สืบราคาจากท้องตลาด
5.3	ค่า Implement Setup and Configuration สำหรับศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า-นางเลิ้ง	1	หน่วย	9,000,000.00	10,212,058.21	สืบราคาจากท้องตลาด
รวมค่าใช้จ่ายอื่นๆ					80,553,210.89	
			รวมทั้งสิ้น		**948,361,321.06**	

8.2 ค่าใช้จ่ายบุคลากร

- ไม่มี

9. สถานที่ติดตั้งใช้งานระบบ /อุปกรณ์

ที่	รายการ	สถานที่ติดตั้ง/ชื่อระบบงาน	กำหนดติดตั้ง (เดือน/ปี)
1	**ระบบสื่อสารข้อมูลภายในและรักษาความปลอดภัยส่วนกลาง**		
1.1	ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.2	ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.3	อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network access control)	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.4	ระบบป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.5	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.6	อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.7	ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.8	อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection)	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.9	ระบบป้องกันภัยคุกคาม Domain Name System	สน.บท ลำลูกกา	กรกฎาคม/2566
1.10	ระบบจัดเก็บข้อมูลและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.11	อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง	สน.บท ลำลูกกา	กรกฎาคม/2566
1.12	อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์	สน.บท ลำลูกกา	กรกฎาคม/2566
1.13	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย	สน.บท ลำลูกกา	กรกฎาคม/2566
1.14	สิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention)	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.15	ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.16	อุปกรณ์ป้องกันเครือข่าย Internet Firewall	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.17	อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application ระหว่างศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า - นางเลิ้ง	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.18	ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network)	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.19	อุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch	สน.บท ลำลูกกา/วังไชยา	
1.20	ห้องปฏิบัติการ Security Operations Center (SOC)	สน.บท ลำลูกกา	กรกฎาคม/2566
1.21	SOC Services Operators 24x7	สน.บท ลำลูกกา	กรกฎาคม/2566
1.22	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
1.23	Implement Setup and Configuration	สน.บท ลำลูกกา/วังไชยา	กรกฎาคม/2566
2	**ระบบคอมพิวเตอร์ส่วนภูมิภาค**		
2.1	ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software)	สำนักทะเบียน	กรกฎาคม/2566
2.2	ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response)	สำนักทะเบียน	กรกฎาคม/2566

10. การฝึกอบรม (หลักสูตร วิธีการฝึกอบรม ระยะเวลา ค่าใช้จ่าย จำนวนผู้ฝึกอบรมและวิทยากร)

- ไม่มี

11. ระยะเวลาดำเนินงาน

11.1 ระยะเวลาดำเนินงานโครงการ

รวม 180 วัน หลังจากลงนามในสัญญา ห้วงเวลาตั้งแต่เมษายน 2566 – เดือนกันยายน 2566

11.2 แผนการดำเนินงานตลอดโครงการ

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															

11.3 การบำรุงรักษา (งบประมาณต่อปี วิธีหรือขั้นตอนการบำรุงรักษา)

- ไม่มี

12. ผลผลิตของโครงการ

12.1 เชิงปริมาณ

- มีระบบที่จัดเก็บและวิเคราะห์ log ได้ไม่น้อยกว่า 30 GB ต่อวัน

12.2 เชิงคุณภาพ

- กรมการปกครองมีระบบรักษาความปลอดภัยทางไซเบอร์ ตามประกาศพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

13. ตัวชี้วัดสัมฤทธิ์ผลด้าน IT

13.1 เชิงปริมาณ (เช่น การลดระยะเวลาในการปฏิบัติงาน การลดงบประมาณ เป็นต้น)

- ติดตั้งระบบรักษาความปลอดภัยทางไซเบอร์ที่สามารถวิเคราะห์ log ได้ไม่น้อยกว่า 30 GB ต่อวัน

13.2 เชิงคุณภาพ (เช่น การเพิ่มประสิทธิภาพ เป็นต้น)

- เพิ่มประสิทธิภาพในการรักษาความปลอดภัยในการให้บริการประชาชน

14. ความพร้อมของหน่วยงาน

14.1 ด้านบุคลากร ICT ที่มีอยู่ในปัจจุบัน

หน่วยงาน/สถานที่	ตำแหน่ง	ระดับ	จำนวน
ส่วนกลาง	ผู้อำนวยการสำนักบริหารการทะเบียน		1
สำนักบริหารการทะเบียน	นักวิชาการคอมพิวเตอร์	เชี่ยวชาญ	1
	นักวิชาการคอมพิวเตอร์	ชำนาญการพิเศษ	4
	นักวิชาการคอมพิวเตอร์	ชำนาญการ/ปฏิบัติการ	13
	เจ้าพนักงานเครื่องคอมพิวเตอร์	ชำนาญงาน	16
รวม			35
ส่วนภูมิภาค			
ศูนย์บริหารการทะเบียนภาค 1-9	นักวิชาการคอมพิวเตอร์	ชำนาญการ	5
และสาขาจังหวัด 77 จังหวัด	เจ้าพนักงานปกครอง	ชำนาญการ	10
	เจ้าพนักงานเครื่องคอมพิวเตอร์	ชำนาญงาน	28
	เจ้าพนักงานธุรการ	ชำนาญงาน	191
	เจ้าหน้าที่ปกครอง	ชำนาญงาน	130
รวม			**364**
รวมทั้งหมด			**399**

14.2 ประเด็นความพร้อมด้านอื่น ๆ (ถ้ามี)

- ไม่มี

15. ประเด็นความเสี่ยงของโครงการและแนวทางการแก้ไข

- ไม่มี

16. กฎหมายที่เกี่ยวข้อง (ถ้ามี)

- ไม่มี

17. ประโยชน์ที่จะได้รับ

17.1 มิติภาคประชาชน

17.1.1 ข้อมูลของประชาชนมีความปลอดภัย

17.2 มิติภาครัฐ

17.2.1 ระบบสารสนเทศมีความเสถียรภาพมากขึ้น

17.2.2 มีระบบป้องกันภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ

ค. การลงนามรับรองโครงการ

1. ผู้จัดทำ / ขออนุมัติโครงการ

ลงชื่อ .....

(นางสาวลักษณา อภิรติปัญญา)

ตำแหน่ง ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

หน่วยงาน สำนักบริหารการทะเบียน กรมการปกครอง

โทรศัพท์ 0-2791-7410 โทรสาร 0-2549-5040

e-Mail : lucksana.ap@gmail.com

2. ผู้ควบคุมโครงการ

ลงชื่อ .....

(นายสันติ รังษิรุจิ)

ตำแหน่ง ผู้อำนวยการสำนักบริหารการทะเบียน

หน่วยงาน กรมการปกครอง กระทรวงมหาดไทย

3. ผู้รับผิดชอบโครงการระดับกระทรวง/กรม

ลงชื่อ .....

(นายสมยศ พุ่มน้อย)

ตำแหน่ง รองอธิบดีกรมการปกครอง ฝ่ายการทะเบียนและเทคโนโลยีสารสนเทศ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

กรมการปกครอง กระทรวงมหาดไทย

4. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกระทรวง

ลงชื่อ .....

(.....)

รองปลัดกระทรวงมหาดไทย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

กระทรวงมหาดไทย

ภาคผนวก ก

ภาคผนวก ก

รายละเอียดคุณลักษณะเฉพาะ (Specification) ของรายการที่จัดหา

โครงการจัดหาระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ กรมการปกครอง

(Security Operations Center: SOC)

ภาคผนวก ก.

1. ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment)

จำนวน 1 ระบบ

คุณสมบัติพื้นฐาน

1.1. เป็นซอฟต์แวร์ออกแบบมาเพื่อตรวจสอบและบริหารจัดการช่องโหว่โดยเฉพาะ ซึ่งสามารถเลือกการตรวจสอบได้ทั้งแบบ Single IP และ IP Range

1.2 สามารถตรวจสอบ (Scan) ช่องโหว่ของระบบดังต่อไปนี้

1.2.1 ระบบปฏิบัติการ (Ope/rating System) ได้แก่ Microsoft Windows, Linux Red Hat, CentOS, Solaris และ VMWare ได้เป็นอย่างน้อย

1.2.2 ระบบฐานข้อมูล (Database) ได้แก่ Microsoft SQL Server, Oracle, MySQL และ DB2 ได้เป็นอย่างน้อย

1.3 สามารถกำหนดสิทธิของผู้ใช้งาน เพื่อเข้าถึงระบบด้วยสิทธิ์ที่ต่างกันได้ (Role-Based Management)

1.4 รองรับการตรวจสอบ (Scan) ทั้งแบบ Non-Credential Scan และ Credential Scan

1.5 มีการจัดลำดับความรุนแรงของช่องโหว่และแสดงรายละเอียดของปัญหา เช่น Malware, Exploit Exposure และ CVSS ได้เป็นอย่างน้อย

1.6 สามารถกำหนดให้ตรวจสอบเฉพาะ Ports ที่ต้องการได้ และได้ทั้ง TCP และ UDP ports (Common Ports)

1.7 สามารถสร้าง และแก้ไขรูปแบบในการตรวจสอบ (Modify Scan Template) ได้

1.8 สามารถให้คำแนะนำหรือวิธีในการแก้ไขปัญหาของช่องโหว่ (Remediation) และแสดงแหล่งที่สามารถดาวน์โหลดซอฟท์แวร์ปรับปรุงแก้ไข (Patch/Hotfix) ต่างๆ รวมถึงมีการประเมินเวลาที่ใช้ในการแก้ปัญหาได้

1.9 สามารถอัพเดตฐานข้อมูลการตรวจสอบช่องโหว่จากผู้ผลิตได้โดยอัตโนมัติ (Automatic) หรือโดยผู้ดูแลระบบ (Manual)

1.10 สามารถตั้งค่าการตรวจสอบล่วงหน้าได้ (Schedule Scan)

2. ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor)

จำนวน 1 ระบบ

ประกอบด้วย

2.1 ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่าย

คุณสมบัติพื้นฐาน

2.1.1 เป็นซอฟต์แวร์ network monitoring ทำหน้าที่ตรวจสอบอุปกรณ์เครือข่าย

2.1.2 มีความสามารถในการตรวจสอบระบบเครือข่ายได้ทั้งอุปกรณ์ที่อยู่บนโครงข่าย (on-premises), cloud services (off-premises) และแบบ Hybrid ด้วยลักษณะการวิเคราะห์ประสิทธิภาพแบบ hop-by-hop รวมถึงสามารถแสดงข้อมูลจำพวก Latency, Packet Drop, AS Number ได้เป็นอย่างน้อย

2.1.3 มี Intelligent Maps ที่แสดงความสัมพันธ์และความเชื่อมโยงของ routers, switches, interfaces, volumes และ groups รวมถึงสามารถ Update ได้แบบอัตโนมัติ

2.1.4 สามารถทำ automate discovery และทำ Map ของอุปกรณ์เครือข่าย, ค่า performance ต่างๆ, link utilization และความครอบคลุมของ wireless (wireless coverage)

2.1.5 รองรับการ monitor อุปกรณ์เครือข่ายที่กรมการปกครองใช้งานอยู่ในปัจจุบัน

2.1.6 สามารถทำการตรวจสอบ, แจ้งเตือน (alert) และออกรายงานเกี่ยวกับ Hardware Health เพื่อตรวจสอบอุปกรณ์เครือข่าย เช่น Power Supply Status, Fan Status หรือ Temperature เป็นต้น

2.1.7 สามารถ monitoring end-user experience ด้วยการทำ Packet Capture and Analysis ที่เกิดจาก application หรือ network ได้

2.1.8 รองรับการเก็บ historical data และนำไปใช้คำนวณ baseline threshold ของอุปกรณ์เครือข่ายได้

2.1.9 สามารถทำรายงานได้ทั้งแบบที่มีรูปแบบอยู่แล้วในระบบ (out-of-the-box) หรือกำหนดจากค่าที่อยู่ในระบบขึ้นเอง (customize) โดยรองรับการตั้งค่าช่วงเวลาได้ (schedule)

2.2 ซอฟต์แวร์วิเคราะห์ Traffic ที่เกิดขึ้นภายในระบบเครือข่าย

คุณสมบัติพื้นฐาน

2.2.1 สามารถวิเคราะห์ประเภทของ flow traffic ดังต่อไปนี้ NetFlow v5/v9, J-Flow, IPFIX, sFlow, Huawei NetStream หรือ Cisco NBAR2 ได้เป็นอย่างน้อย

2.2.2 สามารถใช้งานร่วมกับอุปกรณ์เครือข่ายจาก vendor ต่างๆได้ เช่น Cisco, HP, Juniper, Huawei, Extream, Nortel และ VMware

2.2.3 รองรับ CBQoS, BGP (Border Gateway Protocol)

2.2.4 สามารถตรวจสอบหา application ที่มีการใช้งาน bandwidth สูงสุดได้ รวมถึงสามารถติดตามค่า application traffic ที่ได้รับจาก ports, source IPs, destination IPs หรือ protocols

2.2.5 ต้องสามารถทำงานร่วมกันกับระบบ Network Monitoring System (NMS) หรืออื่นๆ ที่เกี่ยวข้องได้จากหน้าจอเดียว

2.2.6 มีลิขสิทธิ์การใช้งานถูกต้องตามกฎหมาย

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

คุณสมบัติพื้นฐาน

3.1 เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อทำหน้าที่ Network Access Control (NAC) โดยเฉพาะ

3.2 มีความสามารถในการมองเห็น หรือตรวจพบอุปกรณ์ และ user ในเครือข่าย รวมถึงแสดงรายละเอียดอุปกรณ์แบบ headless device ในลักษณะโปรไฟล์ได้

3.3 รองรับการกำหนดนโยบาย (policy) และเปลี่ยนการตั้งค่า (configuration) บนอุปกรณ์ Switch และ Wireless ได้เช่น 3COMS, HP, Aruba, Arista, Cisco, Dell, H3C, Fortinet, Juniper ได้เป็นอย่างน้อย

3.4 สามารถตรวจสอบ (scan) ระบบเครือข่าย เพื่อตรวจจับ และจัดสรรอุปกรณ์ได้ทั้งแบบ Agent และ Agentless และสร้างรายการอุปกรณ์ (Inventory) ที่ตรวจพบบนเครือข่ายได้

3.5 สามารถติดตั้ง และบริหารจัดการได้จากส่วนกลาง (Centralized deployment and management)

3.6 สามารถกำหนด isolate และจำกัดการเข้าถึง VLAN กับอุปกรณ์ที่ตรวจพบการตั้งค่าไม่ตรงกับ compliant หรือข้อกำหนดองค์กรได้

3.7 สามารถทำงานได้แบบ out-of-band โดยไม่ต้องติดตั้งในระบบแบบ in-line เพื่อตรวจสอบ traffic

3.8 สามารถกำหนด policy ตามเงื่อนไข Location, user or host group และตามช่วงเวลา (Schedule) ได้

3.9 สามารถกำหนด portal สำหรับการเชื่อมต่อเครือข่าย และลงทะเบียนได้ โดยสามารถแยกตาม user/host profile ได้

3.10 สามารถทำ policy simulator โดยการจำลอง host, adapter และ user เพื่อทดสอบ policy ก่อนใช้งานจริงได้

4. ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) จำนวน 11,500 ชุด

คุณสมบัติพื้นฐาน

4.1 สามารถบริหารจัดการ การใช้งานกับเครื่องคอมพิวเตอร์ Client และ Server เวอร์ชั่นต่างๆ ดังต่อไปนี้

4.1.1 Windows 10

4.1.2 Windows Server 2012 R2 Server Standard

4.1.3 Windows Server 2016

4.2 มีความสามารถในการทำ Patch Management ได้

4.3 ความสามารถในการทำ Policy Management ได้

4.4 รองรับการทำงานร่วมกับระบบ LDAP หรือ Active Directory ได้

4.5 รองรับการทำ Inventory Management ได้

5. อุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) จำนวน 2 หน่วย

ประกอบด้วย

5.1 ระบบตรวจจับภัยคุกคามทางไซเบอร์บนระบบเครือข่ายด้วยการวางกับดักและเหยื่อล่อ (Deception)

คุณสมบัติพื้นฐาน

5.1.1 เป็นอุปกรณ์ Appliance ที่ออกแบบเฉพาะเพื่อทำหน้าที่ตรวจจับการภัยคุกคามทางไซเบอร์ (Cyber Threats – attacker and malware) โดยสามารถตรวจจับได้ทั้งทางด้าน Network และ Endpoint โดยเฉพาะ

5.1.2 สามารถสร้างกับดักในระบบ Network ได้จำนวนไม่น้อยกว่า 5,000 IP Decoys และรองรับจำนวนเครือข่าย VLAN/Subnet ไม่น้อยกว่า 200 VLANs ทั้งฝั่ง DC/DR

5.1.3 สามารถแสดงรายงาน Attack Forensics ในรูปแบบ STIX, IOC, PCAP และ CSV format ได

5.1.4 สามารถสร้างกับดักล่อในรูปแบบ Real-OS decoy โดย support ทั้ง Windows และ Linux เช่น Ubuntu และ CentOS ได้เป็นอย่างน้อย

5.1.5 สามารถดักจับข้อมูลบนเครือข่ายผ่าน VLAN โดยใช้มาตรฐาน 802.1Q (VLAN trunk)

5.1.6 สามารถกำหนดการสร้างเป้าหมายสำหรับการเป็นกับดักล่อด้วย DHCP และ Static IP Address ได้

5.1.7 สามารถสร้างกับดักแบบอัตโนมัติ (Dynamic) โดยสามารถปรับตามข้อมูล (Learning) จาก Networks/VLAN discovery และ Active Directory ได้ดังนี้

5.1.7.1 ชื่อของ Hostname หรือ DNS Name สอดคล้องกับ Hostname/DNS Name ในเครือข่าย

5.1.7.2 MAC Address สอดคล้องกับข้อมูล Mac Address ในเครือข่าย

5.2 ระบบการวางเหยื่อล่อ (Baits, Breadcrumb) บนเครื่องผู้ใช้งานหรือเครื่องแม่ข่าย และป้องกันข้อมูลจาก Ransomware ร่วมกับระบบวางกับดัก

คุณสมบัติพื้นฐาน

5.2.1 Endpoint ที่มีลิขสิทธิ์ใช้งานถูกต้องตามกฎหมายจำนวนไม่น้อยกว่า 200 Endpoints

5.2.2 สามารถติดตั้งเหยื่อล่อ (Breadcrumbs หรือ False Credential) บนเครื่อง Endpoint และ สามารถปรับปรุงข้อมูลเหยื่อล่อตาม Profile ของกับดักได้

5.2.3 สามารถกำหนดสร้างเหยื่อล่อ (Credential) บนระบบปฏิบัติการ Windows ใน application เช่น Firefox, Google Chrome, Internet Explorer, Windows Explorer (SMB Client), FileZilla, PuTTy, LSASS, Remote Desktop ได้

5.2.4 Endpoint Agent รองรับการติดตั้งบนระบบปฏิบัติการ Windows, Linux และ MacOS ได้

5.2.5 สามารถปรับแต่งการใช้งานของ Client Profile เพื่อกำหนด Feature/Function, กำหนด Service Name, Description, และ การ Upgrade Endpoint Software ได้

5.3 ระบบบริหารจัดการส่วนกลางของระบบตรวจจับภัยคุกคามทางไซเบอร์บนระบบเครือข่ายด้วยการวางกับดักและเหยื่อล่อ

คุณสมบัติพื้นฐาน

5.3.1 เป็นอุปกรณ์ Appliance ขนาด 1U เพื่อใช้ในการบริหารจากส่วนกลางของระบบตรวจจับภัยคุกคามทางไซเบอร์บนระบบเครือข่ายด้วยการวางกับดักและเหยื่อล่อ

5.3.2 มีพอร์ต Ethernet จำนวนไม่น้อยกว่า 2 พอร์ต

5.3.3 มี Power Supply แบบ Hot-Swappable จำนวน 2 หน่วย

5.3.4 ระบบสามารถรวมข้อมูลจากทุกอุปกรณ์ของระบบตรวจจับภัยคุกคามทางไซเบอร์บนระบบเครือข่ายด้วยการวางกับดักและเหยื่อล่อบน Dashboard เดียวกันได้

5.3.5 ระบบสามารถบริหารจัดการอุปกรณ์และปรับแต่ง Configuration ได้จากระบบจัดการส่วนกลาง

6. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) จำนวน 4 หน่วย

คุณสมบัติพื้นฐาน

6.1 เป็นอุปกรณ์ Web Application Firewall (WAF) ที่สามารถป้องกัน Web Application จากภัยคุกคาม ได้

6.2 สามารถรองรับ throughput ไม่น้อยกว่า 5 Gbps

6.3 มีพอร์ตการเชื่อมต่อระบบเครือข่าย (Network Interfaces) อย่างน้อย ดังนี้

6.3.1 แบบ 1G (RJ45) จำนวนไม่น้อยกว่า 8 พอร์ตและสามารถทำงานแบบ Bypass ได้ไม่น้อยกว่า 8 พอร์ต

6.3.2 แบบ 1G (SFP) จำนวนไม่น้อยกว่า 4 พอร์ตแบบ 10G (SFP+) จำนวนไม่น้อยกว่า 4 พอร์ต

6.4 มีพอร์ต Management หรือ Console สำหรับบริหารจัดการอุปกรณ์อย่างน้อย 1 พอร์ต

6.5 มีหน่วยเก็บข้อมูล Storage ขนาด 2 TB ไม่น้อยกว่า 2 หน่วย

6.6 สามมารถป้องกันการโจมตีผ่านทางเว็บไซต์ ได้อย่างน้อยดังนี้

6.6.1 OWASP Top 10

6.6.2 Cross Site Scripting

6.6.3 SQL Injection

6.6.4 Cross Site Request Forgery

6.6.5 Session Hijacking

6.6.6 Web Service Signature

6.7 มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน 2 หน่วย

7. ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response) จำนวน 11,500 หน่วย

คุณสมบัติพื้นฐาน

7.1 สามารถตรวจจับและป้องกันจากภัยคุกคามที่โจมตีเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint) ได้เช่น Ransomware, Trojan, Worm, Virus, Exploit, Rootkit, Malware, Lateral Movement, OSX.Malware, Linux.Malware และ unknown malware เป็นอย่างน้อย

7.2 ระบบต้องมีความสามารถในการตรวจจับและตอบสนองเมื่อระบบตรวจจับเหตุการณ์ผิดปกติด้านความปลอดภัย Endpoint Detection and Response (EDR) ได้ดังต่อไปนี้

7.2.1 สามารถแสดงผล Graphical Process Tree และตารางของเหตุการณ์ที่ถูกภัยคุกคามโจมตี

7.2.2 สามารถแสดงเหตุการณ์ที่ถูกภัยคุกคามโจมตี เช่น ไฟล์ที่ถูกภัยคุกคามสร้างขึ้น (File Creation), ไฟล์ที่ถูกภัยคุกคามแก้ไข (File Modification), ไฟล์ที่ถูกภัยคุกคามลบ (File Deletion), Network Actions, ข้อมูล Process และ Indicator เป็นต้น

7.2.3 ใช้เทคนิค TrueContext หรือ Storyline หรือวิธีการอื่นๆที่เทียบเท่า ในการช่วยเข้าใจเรื่องราว (Story) และสาเหตุที่แท้จริง (root cause) ของเหตุการณ์ด้านความปลอดภัยหลังถูกภัยคุกคามโจมตี ทำให้ตรวจสอบปัญหาที่เกิดขึ้นได้มีประสิทธิภาพ

7.2.4 รองรับการทำ Automated และ Manual ในการ Response เมื่อตรวจสอบพบการโจมตี และสามารถกำหนดการ Action สำหรับเครื่อง Endpoint ได้เช่น Disconnect from Network, Reconnect to Network, Update Software, Shut Down, Reboot, Uninstall, Remote Shell และ View และสามารถกำหนดการ Action สำหรับ Mitigation and Threat ได้เช่น Kill, Quarantine, Unquarantine และ Remediate ได้ หรือวิธีการอื่นที่เทียบเท่า หรือ ดีกว่า

7.2.5 สามารถทำ Full Remote Shell เพื่อให้ Security Team เข้ามาช่วยตรวจสอบการโจมตี และรวบรวมข้อมูล Forensic ในการแก้ไขปัญหา ทำให้ประหยัดเวลาในการช่วยเหลือได้มีประสิทธิภาพ

7.3 ระบบรองรับเทคนิค Static AI ในการใช้ Machine Learning ในป้องกันมัลแวร์ โดยไม่ต้องใช้ฐานข้อมูล (Signature-less) หรือระบบอื่นที่ดีกว่า

7.4 สามารถดาวน์โหลด ไฟล์ที่ต้องสงสัย หรือ Threat file เพื่อนำมาวิเคราะห์ภายหลังได้

7.5 ระบบสามารถตรวจจับการโจมตีแบบ fileless และ command line exploits เช่น การโจมตีผ่าน powershell command line ได้

8. อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)

จำนวน 2 หน่วย

คุณสมบัติพื้นฐาน

8.1 เป็นอุปกรณ์ประเภท Hardware Appliance เพื่อใช้ในการตรวจจับและป้องกัน SPAM และ Virus ของ E-Mail โดยเฉพาะ

8.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T (RJ-45) จำนวนไม่น้อยกว่า 4 ช่อง และแบบ SFP Gigabit Ethernet จำนวนไม่น้อยกว่า 2 ช่อง

8.3 มีพื้นที่เก็บข้อมูล (Storage) ขนาด 2 TB จำนวนไม่น้อยกว่า 2 หน่วย และรองรับการทำ RAID 0, 1, 5, 10 เป็นอย่างน้อย

8.4 มีแหล่งจ่ายไฟแบบ Dual Power Supplies ที่สามารถใช้งานกับระบบไฟฟ้าในประเทศไทยแบบ 220 V. AC, 50 Hz. ได้

8.5 สามารถตรวจจับและป้องกันภัยคุกคามทางอีเมล์ ได้แก่ Spam, Malware, Bulk email, Ransomware, Phishing, Business Email Compromise (BEC) ได้ทั้งขาเข้าและขาออก (Inbound & Outbound) จำนวนไม่น้อยกว่า 500 Domains

9. ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)

จำนวน 1 ระบบ

ประกอบด้วย

9.1 ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

คุณสมบัติพื้นฐาน

9.1.1 เป็นระบบที่ออกแบบมาโดยเฉพาะเพื่อทำหน้าที่ควบคุมความปลอดภัยในการใช้งาน Privileged Account โดยสามารถบริหารจัดการรหัสผ่าน และควบคุมเฝ้าระวังการใช้งาน Privileged Session เพื่อลดความเสี่ยงจากการถูกโจมตี และสามารถตอบโจทย์ตามความต้องการของ Compliance ได้

9.1.2 ผลิตภัณฑ์ที่นำเสนอจะต้องได้รับการรับรองอยู่ในกลุ่ม Leader ด้าน Privileged Access Management จากหน่วยงานที่ทำการวิจัยตลาดชั้นนำ (Gartner) ในปี 2020 เป็นอย่างน้อย

9.1.3 ต้องมีลิขสิทธิ์สำหรับผู้ใช้งานระบบจำนวนไม่น้อยกว่า 50 ผู้ใช้งาน (Users) โดยสามารถบริหารจัดการรหัสผ่านได้ไม่จำกัดจำนวน Target devices และสามารถทำการบันทึกการใช้งาน (Session Recording) ได้ไม่จำกัดจำนวน Target devices

9.1.4 สามารถตรวจสอบและวิเคราะห์ภัยคุกคามจากพฤติกรรมการใช้งาน (Privileged Threat Analytics) ได้ไม่จำกัดจำนวน Target devices

9.1.5 สามารถเข้ารหัสข้อมูลของ Privileged Account ด้วย Algorithm แบบ AES-256, RSA-2048 หรือดีกว่า โดยผ่านการรองรับมาตรฐาน FIPS 140-2

9.2 ระบบตรวจสอบยืนยันตัวตนผู้ใช้งานแบบสองชั้น (Two Factor Authentication)

คุณสมบัติพื้นฐาน

9.2.1 เป็นระบบ Software สำหรับทำหน้าที่บริหารจัดการระบบตรวจสอบยืนยันตัวตนแบบ 2 ชั้น (Two-factor Authentication) โดยใช้ One-time Password ในการยืนยันตัวตน

9.2.2 ระบบ Software บริหารจัดการ สามารถรองรับการติดตั้ง ดังต่อไปนี้

9.2.2.1 รองรับการติดตั้งบนระบบปฏิบัติการ Windows Server 2012, Windows Server 2012 R2 และ Windows Server 2016 ได้เป็นอย่างน้อย

9.2.2.2 รองรับการเชื่อมต่อกับระบบฐานข้อมูล เช่น PostgreSQL หรือ MySQL หรือ Microsoft SQL ได้

9.2.2.3 รองรับการเชื่อมต่อกับ LDAP Directories เช่น Active Directory, Open LDAP ได้เป็นอย่างน้อย

9.2.2.4 รองรับ RADIUS Authentication Protocols เช่น PAP และ MSCHAPv2 ได้

9.2.3 ระบบที่เสนอต้องมี Soft Token ที่ได้รับมาตรฐานความปลอดภัย FIPS 140-2

9.2.4 ระบบต้องสามารถทำงานในรูปแบบ Redundancy หรือ Fail Over ได้

9.2.5 ระบบบริหารจัดการต้องมีหน้าเว็บบริการตนเอง (User Self Service Portal)

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

คุณสมบัติพื้นฐาน

10.1 เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อป้องกันการโจมตีแบบ DDoS โดยเฉพาะ

10.2 มีความเร็วในการตรวจจับการโจมตี (Throughput) ไม่น้อยกว่า 5 Gbps และรองรับ Packets Rate ไม่น้อยกว่า 2,500,000 pps (Packets per Second)

10.3 รองรับ Concurrent Sessions ได้สูงสุด 8,000,000 Sessions

10.4 มีพอร์ต 1 GE แบบ Copper Bypass อย่างน้อย 4 พอร์ต และรองรับพอร์ต 1/10 GE (SFP+) อย่างน้อย 4 พอร์ต

10.5 มีพอร์ต Management Port อย่างน้อย 1 พอร์ต และมี Console Port อย่างน้อย 1 พอร์ต

10.6 สามารถป้องกันการโจมตีแบบ Flood Attack ตามประเภทต่อไปนี้ SYN cookies, SYN authentication, ACK authentication, Spoof detection, SSL authentication, DNS authentication, HTTP challenge, TCP/UDP/ICMP flood protection และ Application flood

11. ระบบป้องกันภัยคุกคาม Domain Name System จำนวน 500 หน่วย

คุณสมบัติพื้นฐาน

11.1 ระบบที่นำเสนอเป็นแบบ On-Premise หรือ Cloud Service ที่ออกแบบมาเพื่อทำหน้าที่เป็น Recursive DNS พร้อมบริการด้านความปลอดภัยโดยเฉพาะ

11.2 สามารถรองรับจำนวนผู้ใช้งานไม่น้อยกว่า 500 ผู้ใช้งานได้เป็นอย่างน้อย

11.3 สามารถตรวจจับการเชื่อมต่อและป้องกันภัยคุกคามที่เกิดขึ้นกับระบบโดเมนเนม (Domain Name Server: DNS) ได้ดังนี้เป็นอย่างน้อย

11.4 การเชื่อมต่อโดเมนเนม หรือ IP Address ที่ต้องสงสัยว่าเป็นมัลแวร์, Ransomware, Phishing, C&C เป็นอย่างน้อย

11.5 การเชื่อมต่อลักษณะ Domain Generation Algorithm (DGA) ของมัลแวร์

11.6 การเชื่อมต่อไปยัง Hostname และ โดเมน เพื่อตรวจจับการขุดสกุลเงินดิจิตอล (Cryptocurrency hostname and domain)

11.7 สามารถวิเคราะห์ข้อมูล DNS Queries ด้วย Machine Learning เพื่อตรวจจับและป้องกันการขโมยข้อมูลผ่าน DNS (DNS-based data exfiltration), DGA (Domain Generation Algorithm), DNSMessenger และ fast-flux ได้

11.8 สามารถตรวจจับและป้องกันโดยทำงานร่วมกับฐานข้อมูล Threat Intelligence ที่เป็นผลิตภัณฑ์เดียวกับ ระบบตรวจจับฯ ที่นำเสนอ โดยมีฐานข้อมูลจากแหล่งอื่น (Threat Intelligence) ไม่น้อยกว่า 10 แหล่ง

11.9 มีข้อมูล Threat Intelligence Feeds ไม่น้อยกว่า 15 Threat Feeds

11.10 สามารถทำ DNSSEC Validation ได้

11.11 สามารถกำหนดเงื่อนไขนโยบายความปลอดภัย(Security Policy)ในการตอบ DNS query โดยกำหนดให้ Block หรือ Redirect ได้

12. ระบบจัดเก็บข้อมูลและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM) จำนวน 1 ระบบ

ประกอบด้วย

12.1 ระบบเก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่าย

คุณสมบัติพื้นฐาน

12.1.1 เป็นอุปกรณ์ Software ที่ออกแบบเฉพาะสำหรับเก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่ายโดยทำหน้าที่เป็น Log Management โดยเฉพาะ

12.1.2 ระบบที่เสนอมีการทำงานเป็นแบบ Distributed Architecture โดยมีการติดตั้งอุปกรณ์ที่ทำหน้าที่เก็บบันทึกข้อมูลทางด้านการรักษาความปลอดภัยเครือข่าย (Log Management) แยกจากอุปกรณ์ที่ทำหน้าที่วิเคราะห์และบริหารจัดการข้อมูลความปลอดภัยเครือข่าย (Security Information and Event Management: SIEM) เพื่อประสิทธิภาพในการทำงานที่ดี และต้องเป็นผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกัน

12.1.3 สามารถรองรับอุปกรณ์ที่จัดเก็บ Log ได้ไม่จำกัด เพื่อให้สามารถเก็บ Log จากอุปกรณ์ต้นทางในอนาคตโดยไม่มีค่าใช้จ่ายเพิ่มเติม

12.1.4 สามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลการใช้งาน (Raw Log) ที่ได้จากอุปกรณ์โดยรองรับปริมาณข้อมูลได้ไม่น้อยกว่า 2,500 เหตุการณ์ต่อวินาที (Event per second) หรือ 500 GB ต่อวัน

12.1.5 สามารถทำการส่งต่อ (Forwarding) log ไปยังอุปกรณ์ Log Server อื่นๆ หรืออุปกรณ์ SIEM ได้

12.2 ระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร

คุณสมบัติพื้นฐาน

12.2.1 เป็นผลิตภัณฑ์ที่ใช้สำหรับวิเคราะห์เหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management) โดยเฉพาะ

12.2.2 ระบบที่เสนอมีการทำงานเป็นแบบ Distributed Architecture โดยติดตั้งอุปกรณ์สำหรับเก็บและบริหารจัดการข้อมูลการใช้งานเครือข่าย (Log Management) แยกจากอุปกรณ์สำหรับวิเคราะห์เหตุการณ์ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ (Security Information and Event Management) โดยใช้ผลิตภัณฑ์ที่มีเครื่องหมายการค้าเดียวกัน

12.2.3 สามารถรับปริมาณ Log ได้ไม่น้อยกว่า 1000 เหตุการณ์ต่อวินาที (Events per Second)

12.2.4 สามารถเชื่อมโยงเหตุการณ์จาก Source ต่างๆ เข้าด้วยกัน (Correlation) ทั้งแบบ Real-time และ Historical เพื่อหาต้นตอของภัยคุกคาม และสามารถ Customize เพิ่มเติมได้

12.2.5 สามารถสร้างความสัมพันธ์ของเหตุการณ์หลายๆ เหตุการณ์ในรูปแบบแผนภาพ (Event Graph) แบบหลายลำดับชั้น เพื่อใช้ในการเฝ้าระวังเหตุการณ์แบบ Real-time และวิเคราะห์ย้อนหลัง (Historical) ได้

13. อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง **จำนวน 1 หน่วย**

คุณสมบัติพื้นฐาน

13.1 เป็นอุปกรณ์แบบ Hardware Appliance ทำหน้าที่ตรวจจับภัยคุกคามขั้นสูงโดยเฉพาะ

13.2 รองรับ Sniffer Throughput ได้อย่างน้อย 4 Gbps

13.3 รองรับ Sandbox Pre-Filter Throughput ได้อย่างน้อย 12,000 File per Hour

13.4 รองรับ VM Sandboxing Throughput ได้อย่างน้อย 480 File per Hour

13.5 สามารถติดตั้งแบบ Standalone เพื่อรับ sample จากช่องทางดังนี้ได้

13.5.1 Spanned Switch port

13.5.2 Network Taps

13.5.3 Email BCC

13.5.4 On-demand URL and File upload

13.5.5 Network file share

13.6 อุปกรณ์ที่เสนอสามารถตรวจสอบไฟล์ที่ทำงานในลักษณะ Virtual Machine ได้จำนวนอย่างน้อย 24 ชุด พร้อมกัน

13.7 อุปกรณ์ที่เสนอต้องมีเทคนิค Anti-Evasion เช่น Sleep calls, Process และ Registry queries เป็นอย่างน้อย

13.8 อุปกรณ์ที่เสนอสามารถตรวจสอบ Callback Detection เช่น Malicious URL visits, botnet C&C communication ได้เป็นอย่างน้อย

13.9 อุปกรณ์ที่เสนอสามารถตรวจสอบไฟล์นามสกุลต่าง ๆ เช่น .apk, .bat, .cab, .cmd, .dll, .dmg, .doc, .docx, .elf, .exe, .gz, .html, .iso, .jar, .js, .msi, .pdf, .ppt, .pptx, .rar, .rtf, .swf, .tar, .tgz, .vbs, WEBLink, .xls, .xlsx, .zip ได้เป็นอย่างน้อย

14. อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ จำนวน 1 หน่วย

คุณสมบัติพื้นฐาน

14.1 เป็นอุปกรณ์แบบ appliance ที่ออกแบบมาทำหน้าที่เป็นนักวิเคราะห์ความปลอดภัยเสมือน (Virtual Security Analyst) เพื่อระบุ คัดกรอง และตอบสนองต่อมัลแวร์ที่พรางตัวได้

14.2 มีคุณสมบัติ Deep Neural Networks เพื่อสนับสนุนการทำงานแบบ AI และโครงข่ายประสาทเทียม ใช้สนับสนุน

14.3 สามารถลดเวลาในการตรวจสอบ และตรวจจับมัลแวร์จากระดับนาที เป็นระดับวินาที หรือดีกว่าได้

14.4 มี AI ที่ประกอบด้วยคุณลักษณะมัลแวร์ไม่น้อยกว่า 6 ล้านรายการ เพื่อใช้สนับสนุนการตัดสินมัลแวร์ได้ทันทีที่ติดตั้ง พร้อมความสามารถในการเรียนรู้คุณลักษณะใหม่ได้

14.5 เป็นการทำงานแบบ on-premise

14.6 สามารถวิเคราะห์ไฟล์ได้ทั้งแบบ known และ unknown รวมถึงภัยคุกคามในลักษณะ fileless

14.7 สามารถทำงานร่วมกับระบบป้องกันภัยคุกคามเครือข่าย NGFW ภายใต้แบรนด์เดียวกัน เพื่อ quarantine ภัยคุกคามที่เกิดขึ้นได้แบบอัตโนมัติ และ NGFW ดังกล่าวต้องได้รับการยอมรับเป็น Leader

14.8 สนับการทำงานกับไฟล์ และโปรโตคอล ดังต่อไปนี้เป็นอย่างน้อย

14.8.1 Portable Executables (PE) ได้แก่ DLLs, ZIP

14.8.2 Web based ได้ HTML, Javascripts, VBS, VBA, Office documents, PDFs

14.8.3 รองรับโปรโตคอล HTTP และ SMBv2 จากการ sniffer ได้เป็นอย่างน้อย

14.8.4 กรณีทำงานร่วมกับ NGFW ภายใต้แบรนด์เดียวกัน สามารถทำงานร่วมกันเพื่อรับทราฟฟิค HTTP, HTTPS (with SSL decryption), SMTP, POP3, IMAP, MAPI และ FTP

14.8.5 รอบรับการอัพโหลดแบบ Manual/REST API ได้แก่ .tar, .gz, .tar.gz, .zip, .bz2 และ .ra

14.9 สามารถติดตั้งแบบ Sniff mode, manual upload และ API submission

15. อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย จำนวน 1 หน่วย

คุณสมบัติพื้นฐาน

15.1 เป็นอุปกรณ์ Hardware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) ที่เกิดขึ้นบนอุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ของสำนักบริหารการทะเบียน หรืออุปกรณ์รักษาความปลอดภัยเว็บไซต์ (Web Application Firewall) ที่เสนอมาในโครงการได้

15.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1 GE จำนวนไม่น้อยกว่า 2 พอร์ต และมีช่องสำหรับใส่ Transceiverแบบ 25 GE SFP28 จำนวนไม่น้อยกว่า 2 ช่อง

15.3 มี Storage ขนาด 4 TB จำนวนไม่น้อยกว่า 16 หน่วย พร้อมมีคุณบัติ Hard drive Hot Swappable

15.4 รองรับการทำ RAID 0/1/5/6/10/50/60 ได้เป็นอย่างน้อย และมีความจุ หลังทำ RAID สูงสุด ไม่น้อยกว่า 5 TB

15.5 มีอัตราความสามารถในการจัดเก็บข้อมูลเพื่อวิเคราะห์ได้ไม่น้อยกว่า 42,000 Logs/Events per second และสามารถรองรับจำนวน log ได้ไม่น้อยกว่า 3,000 GB ต่อวัน

15.6 รองรับการทำงานร่วมกับ Device หรือ Virtual Domain ได้สูงสุดไม่น้อยกว่า 4,000 devices/Virtual Domain หรือ Virtual System

15.7 รองรับการออกรายงานย้อนหลังในรูปแบบกราฟ หรือชาร์ต เพื่อแสดงการใช้งาน SD-WAN เช่น การใช้งาน applications, latency, packet loss, Jitter ได้เป็นอย่างน้อย หรือมีคุณสมบัติเทียบเท่า หรือดีกว่า

15.8 มี dashboard แสดงผลทั้งแบบ NOC (Network Operations Center) และ SOC (Security Operations Center) เพื่อรองรับการแสดงผล monitoring network security, compromised hosts, vulnerabilities, Security Fabric และ system performance ได้เป็นอย่างน้อย

15.9 สามารถบริหารจัดการอุปกรณ์ผ่านโปรโตคอล HTTPS ผ่าน Web Browser ได้โดยตรง โดยไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติม และโปรโตคอล SSH ได้เป็นอย่างน้อย

15.10 มี Dashboard ที่สรุปข้อมูล Top sources, Top destinations, Top applications, Top websites, Top threats, System events และ Resource usage ได้เป็นอย่างน้อย

16. ลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) จำนวน 1000 หน่วย

คุณสมบัติพื้นฐาน

16.1 สามารถทำงานร่วมกับระบบ internet proxy gateway ของสำนักบริหารการทะเบียน ได้

16.2 สามารถกำหนดนโยบายการใช้งานให้กับผู้ใช้แบบบุคคลหรือกลุ่ม จาก Directory Service เช่น Active Directory หรือ LDAP ได้

16.3 สามารถป้องกันการรั่วไหลข้อมูลสำคัญที่ถูกส่งออกผ่านทางโปรโตคอล FTP, HTTP, HTTPS (Web DLP) ได้ โดยมี Pre-defined Policy ไม่น้อยกว่า 1,000 Policies และครอบคลุมถึง PCI, PII, SOX, HIPAA

16.4 สามารถทำการป้องกันข้อมูลรั่วไหล หากมีการส่งไฟล์รูปภาพที่มีข้อความ Text ปรากฏในรูปภาพผ่านทาง Web post โดยการแปลงข้อความที่ปรากฏเป็น Key Phase เพื่อตรวจสอบร่วมกับ DLP Policy ที่กำหนดไว้ด้วยเทคโนโลยี Optical Characteristic Recognition (OCR) ได้

16.5 สามารถกำหนดนโยบาย และ action ที่เกิดขึ้นตามระดับความเสี่ยงของข้อมูลที่ตรวจพบ เช่น Block, Notify, Audit ได้

17 ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone จำนวน 2 หน่วย

คุณสมบัติพื้นฐาน

17.1 เป็น Software ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่าง ๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล

17.2 สามารถจัดเก็บข้อมูลได้ตามหลักเกณฑ์ การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

17.3 เป็นระบบจัดเก็บข้อมูล Log ที่ได้ผ่านการตรวจสอบคุณสมบัติตามมาตรฐาน "ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์" ได้ตามมาตรฐาน Standard NTS 4003.1-2560

17.4 มีความสามารถบริหารจัดการแบบ Web Base Administration ผ่าน HTTPS และ Command Line Interface (CLI) ผ่าน SSH เพื่อสามารถเข้าไปบริหารจัดการ ระบบ log ผ่านเครือข่ายได้

17.5 ผลลัพธ์ที่ได้จากการค้นหา สามารถส่งออก (Export) เป็นไฟล์รูปแบบ CSV ได้

18 อุปกรณ์ป้องกันเครือข่าย Internet Firewall จำนวน 4 หน่วย

คุณสมบัติพื้นฐาน

18.1 เป็นอุปกรณ์ Next Generation Firewall ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content โดยเฉพาะ แบบ Chassis ที่แยกหน่วยประมวลผลสำหรับการบริหารจัดการ (Control Plane) และ หน่วยประมวลผลสำหรับการจัดการข้อมูล (Data Plane) ออกจากกันภายในตัวอุปกรณ์ ในระดับสถาปัตยกรรม Hardware

18.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) อย่างน้อยดังนี้

18.3 ช่องเชื่อมต่อแบบ 100/1000/10G Cu หรือดีกว่า ไม่น้อยกว่า 4 ช่อง

18.4 ช่องเชื่อมต่อแบบ 1G/10G SFP/SFP+ หรือดีกว่า ไม่น้อยกว่า 12 ช่อง นำเสนอพร้อมโมดูล 10G SPF+ SR ไม่น้อยกว่า 12 โมดูล

18.5 ช่องเชื่อมต่อแบบ 40G/100G QSFP28 หรือดีกว่า ไม่น้อยกว่า 2 ช่อง

18.6 มี Firewall Throughput ไม่น้อยกว่า 100 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

18.7 มี Threat Prevention Throughput หรือ Threat Protection Throughput ไม่น้อยกว่า 74 Gbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

18.8 มีแหล่งจ่ายไฟฟ้า (Power Supply) ไม่น้อยกว่า 4 หน่วย

18.9 มีระบบสำหรับการบริหารจัดการแบบรวมศูนย์ (Centralized Management Firewall) ในรูปแบบ Software หรือ Virtual Appliance ที่ออกแบบมาเพื่อบริหารจัดการอุปกรณ์รักษาความปลอดภัยระดับแอพพลิเคชั่น (Application Firewall) โดยเฉพาะ และมีเครื่องหมายการค้าเดียวกับอุปกรณ์ที่นำเสนอ เพื่อสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ

19 อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application ระหว่างศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า-นางเลิ้ง จำนวน 4 หน่วย

คุณสมบัติพื้นฐาน

19.1 เป็นอุปกรณ์ที่ออกแบบมาสำหรับทำ Application Delivery Control และ Application Security โดยเฉพาะ

19.2 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) 10 Gigabit แบบ SFP+ ไม่น้อยกว่า 8 พอร์ต

19.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 40 Gigabit Fiber Ports (QSFP+) ไม่น้อยกว่า 4 พอร์ต

19.4 มีความสามารถในการทำ L4 Throughput ได้ไม่น้อยกว่า 80 Gbps และ L7 Throughput ไม่น้อยกว่า 40 Gbps

19.5 มี Software หรือ Hardware สำหรับวิเคราะห์ Log และทำ Report หรือ Dashboard สำหรับระบบ Application Diliverly Controller และ Application Security

20 ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network)

จำนวน 2 หน่วย

คุณสมบัติพื้นฐาน

20.1 เป็นอุปกรณ์ Appliance ที่ออกแบบขึ้นมาเฉพาะ เพื่อทำหน้าที่เป็น Next Generation Firewall

20.2 มีเชื่อมต่อระบบเครือข่ายแบบ Gigabit Ethernet(RJ-45) ไม่น้อยกว่า 8 ช่อง และแบบ Gigabit Fiber (SFP) ที่รองรับการติดตั้ง SFP Transceivers ไม่น้อยกว่า 8 ช่อง และแบบ Ten Gigabit Fiber (SFP+) ที่รองรับการติดตั้ง SFP+ Transceivers ไม่น้อยกว่า 2 ช่อง

20.3 สามารถทำการเชื่อมโยง SSL VPN จากเครื่อง Client ไม่น้อยกว่า 5,000 Users

20.4 สามารถรองรับการทำงานแบบ Two Factor Authentication ได้โดยไม่ต้องติดตั้ง Token Serve

20.5 อุปกรณ์รองรับแหล่งจ่ายไฟแบบ Redundant Power Supply (Hot Swap)

20.6 อุปกรณ์มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model

20.7 สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้ เป็นอย่างน้อย

20.8 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10/25 Gigabit Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง

20.9 มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) 40Gbps แบบ QSFP+ หรือ QSFP28 จำนวนไม่น้อยกว่า 4 ช่อง

20.10 มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง

21 กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch จำนวน 4 หน่วย

คุณสมบัติพื้นฐาน

21.1 คุณสมบัติพื้นฐานมีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model

21.2 สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้ เป็นอย่างน้อย

21.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 1/10/25 Gigabit Ethernet หรือดีกว่า จำนวนไม่น้อยกว่า 24 ช่อง

21.4 มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) 40Gbps แบบ QSFP+ หรือ QSFP28 จำนวนไม่น้อยกว่า 4 ช่อง

21.5 มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง

22 ห้องปฏิบัติการ Security Operations Center (SOC)

คุณสมบัติพื้นฐาน

22.1 ปรับปรุงห้องตามที่สำนักบริหารการทะเบียนกำหนดเพื่อใช้เป็นห้องปฏิบัติการ Security Operations Center (SOC)

22.2 ติดตั้งอุปกรณ์ Smart Board หรือ Interactive Board ที่มีคุณสมบัติเป็น Interactive ขนาดหน้าจอไม่น้อยกว่า 50 นิ้ว จำนวน 1 เครื่อง

22.3 ติดตั้ง Display Wall หรือ ติดตั้ง LED TV ขนาดไม่ต่ำกว่า 50 นิ้ว จำนวนไม่น้อยกว่า 8 เครื่อง

22.4 มีระบบควบคุมการแสดงผลออกไปยัง Display Wall หรือ LED TV ที่ติดตั้งได้

22.5 ติดตั้งระบบ Biometric access controlสำหรับเข้าห้องปฏิบัติการ Security Operations Center (SOC)

23. บริการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ SOC Services Operators (ทำงาน 24 ชั่วโมง x 7 วัน)

คุณสมบัติพื้นฐาน

23.1 เฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์
พร้อมให้บริการให้คำปรึกษาผ่านทางอีเมลและโทรศัพท์ตลอด 24 ชั่วโมง

23.2 ดำเนินการจัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ (Log) จำนวนไม่น้อยกว่า 50 IP Address และปริมาณของ Log รวมกันทั้งหมดไม่เกิน 30 GB/Day เป็นระยะเวลาอย่างน้อย 90 วัน

23.3 จัดเตรียมระบบสืบค้นข้อมูลจราจรทางคอมพิวเตอร์ (Log)

23.4 จัดทำรายงานเหตุการณ์ที่อยู่ในข่ายภัยคุกคามทางไซเบอร์ (Cybersecurity Event Report) โดยอยู่ในรูปแบบ Correlation Report
ซึ่งประกอบไปด้วยแผนภูมิรูปภาพตารางแสดงสรุปเหตุการณ์อย่างละเอียด (Correlation Graph) รวมทั้งข้อมูลประกอบที่จำเป็นครบถ้วน พร้อมคำแนะนำ

23.5 จัดทำรายงานเหตุการณ์ผิดปกติที่ยังไม่อยู่ในข่ายภัยคุกคามทางไซเบอร์ (Cybersecurity Informative Report)

24. อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง จำนวน 4 หน่วย

คุณสมบัติพื้นฐาน

24.1 มีลักษณะการทำงานไม่น้อยกว่า Layer 3 ของ OSI Model

24.2 สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIPv2, OSPF ได้เป็นอย่างน้อย

24.3 มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10 Gbps Base-T หรือดีกว่า จำนวนไม่น้อยกว่า 48 ช่อง

24.4 มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) 40Gbps แบบ QSFP+ หรือ QSFP28 จำนวนไม่น้อยกว่า 4 ช่อง

24.5 มีสัญญาณไฟแสดงสถานะของการทางานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง

ภาคผนวก ข

ADVANCED INFORMATION TECHNOLOGY PUBLIC CO.,LTD.
Mobile: 66(06)-3546-1463
Office: 66(0)-2275-9400
Fax: 66(0)-2275-9100
E-mail : eakchai@ait.co.th

ใบเสนอราคา

เลขที่ 2110001/10

เรียน : อธิบดีกรมการปกครอง

: กรมการปกครอง

วันที่ 27 ตุลาคม 2564

เรื่อง : โครงการระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center : SOC)

โทร

แฟกซ์

ลำดับที่	รายการ	จำนวน	ราคาต่อหน่วย	รวม
	โครงการระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center : SOC)			
1	ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment) ยี่ห้อ F-Secure รุ่น F-Secure Radar	1	1,372,000.00	1,372,000.00
2	ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor) ยี่ห้อ WhatsUp Gold รุ่น WhatsUp Gold Premium	1	350,000.00	350,000.00
3	อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC : Network access control) ยี่ห้อ ForeScout รุ่น CounterACT CT-4000	2	1,500,000.00	3,000,000.00
4	ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) ยี่ห้อ ManageEngine รุ่น Desktop-central	11500	850.00	9,775,000.00
5	อุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) ยี่ห้อ acalvio รุ่น ShadowPlex	2	15,587,200.00	31,174,400.00
6	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ยี่ห้อ imperva รุ่น SecureSphere x8520	4	5,599,600.00	22,398,400.00
7	ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR : Endpoint Detection and Response) ยี่ห้อ vmware รุ่น VMware Carbon Black® EDR™	11500	3,360.00	38,640,000.00
8	อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway) ยี่ห้อ Sophos รุ่น Sophos Email Security	2	1,195,300.00	2,390,600.00
9	ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management) ยี่ห้อ CyberArk รุ่น Privileged Access Security	1	37,270,816.37	37,270,816.37
10	อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection) ยี่ห้อ Checkpoint รุ่น 8412 DDoS Protector Appliance	4	5,981,725.00	23,926,900.00
11	ระบบป้องกันภัยคุกคาม Domain Name System ยี่ห้อ BlueCat รุ่น BlueCat Security	500	3,800.00	1,900,000.00
12	ระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM) ยี่ห้อ McAfee รุ่น McAfee Enterprise Security Manager X11 - security appliance	1	28,500,000.00	28,500,000.00
13	อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง ยี่ห้อ Check Point รุ่น SandBlast Threat Emulation Sandboxing	1	9,700,000.00	9,700,000.00
14	อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ ยี่ห้อ Darktrace รุ่น Cyber AI Analyst	1	15,796,000.00	15,796,000.00
15	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย ยี่ห้อ Palo Alto networks รุ่น Panorama M-600	1	5,679,900.00	5,679,900.00
16	ลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) ยี่ห้อ Solarwind รุ่น Data loss prevention	1000	4,500.00	4,500,000.00
17	ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone ยี่ห้อ Softnix รุ่น SOFTNIX LOGGER	2	1,780,000.00	3,560,000.00
18	อุปกรณ์ป้องกันเครือข่าย Internet Firewall ยี่ห้อ Palo Alto รุ่น PA-5450	4	22,338,000.00	89,352,000.00
19	อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application ยี่ห้อ F5 รุ่น BIG-IP i7800 DDOS + Firewall + GSLB	4	8,850,000.00	35,400,000.00

ลำดับที่	รายการ	จำนวน	ราคาต่อหน่วย	รวม
20	ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network) ยี่ห้อ Cisco รุ่น FirePOWER 2140 NGFW	2	2,196,400.00	4,392,800.00
21	อุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switchยี่ห้อ Cisco รุ่น Catalyst 9500-24Y4C	4	1,994,000.00	7,976,000.00
22	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง ยี่ห้อ Cisco รุ่น Nexus 9372TX	4	1,155,000.00	4,620,000.00
23	ห้องปฏิบัติการ Security Operations Center (SOC)	1	2,500,000.00	2,500,000.00
24	SOC Services Operators 24x7 ระยะเวลา 12 เดือน	12	900,000.00	10,800,000.00
25	ค่า Implement Setup and Configuration สำหรับศูนย์ประมวลผลคอมพิวเตอร์ตลองเก้า - นางเลิ้ง	1	9,000,000.00	9,000,000.00
			Total (Baht)	403,974,816.37

หมายเหตุ

1. ยืนราคา : 90 วัน นับถัดจากวันที่เสนอราคา
2. ภาษีมูลค่าเพิ่ม : ราคารวมภาษีมูลค่าเพิ่มแล้ว
3. ติดตั้ง : รวมค่าติดตั้งแล้ว
4. ส่งมอบ : 180 วัน นับถัดจากวันลงนามในสัญญา
5. ประกัน : 1 ปี นับถัดจากวันตรวจรับเสร็จสิ้นสมบูรณ์

ด้วยความเคารพอย่างสูง

(นายเอกชัย เชโหง่ว)

ฝ่ายขาย

ADVANCED INFORMATION TECHNOLOGY PUBLIC CO.,LTD.
Mobile: 66(06)-3546-1463
Office: 66(0)-2275-9400
Fax: 66(0)-2275-9100
E-mail : eakchai@ait.co.th

ใบเสนอราคา

เลขที่ 2110001/11

เรียน : อธิบดีกรมการปกครอง

: กรมการปกครอง

วันที่ 27 ตุลาคม 2564

เรื่อง : โครงการบำรุงรักษาระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center : SOC)

โทร

แฟกซ์

ลำดับที่	รายการ	จำนวน	ราคาต่อหน่วย	รวม
	โครงการบำรุงรักษาระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center : SOC)			
1	MA 1 ปีสำหรับซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment)	1	617,400.00	617,400.00
2	MA 1 ปีสำหรับซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor)	1	350,000.00	350,000.00
3	MA 1 ปีสำหรับอุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC : Network access control)	1	600,000.00	600,000.00
4	MA 1 ปีสำหรับซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software)	1	7,820,000.00	7,820,000.00
5	MA 1 ปีสำหรับอุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution)	1	3,117,440.00	3,117,440.00
6	MA 1 ปีสำหรับอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	1	8,959,360.00	8,959,360.00
7	MA 1 ปีสำหรับระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR : Endpoint Detection and Response)	1	11,592,000.00	11,592,000.00
8	MA 1 ปีสำหรับอุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)	1	956,240.00	956,240.00
9	MA 1 ปีสำหรับระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management)	1	6,000,000.00	6,000,000.00
10	MA 1 ปีสำหรับอุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection)	1	4,785,380.00	4,785,380.00
11	MA 1 ปีสำหรับระบบป้องกันภัยคุกคาม Domain Name System	1	1,900,000.00	1,900,000.00
12	MA 1 ปีสำหรับระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)	1	3,705,000.00	3,705,000.00
13	MA 1 ปีสำหรับระบบอุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง	1	970,000.00	970,000.00
14	MA 1 ปีสำหรับอุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์	1	3,159,200.00	3,159,200.00
15	MA 1 ปีสำหรับอุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย	1	1,703,970.00	1,703,970.00
16	MA 1 ปีสำหรับลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention)	1	1,200,000.00	1,200,000.00
17	MA 1 ปีสำหรับระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า Internet zone	1	712,000.00	712,000.00
18	MA 1 ปีสำหรับอุปกรณ์ป้องกันเครือข่าย Internet Firewall	1	23,200,000.00	23,200,000.00
19	MA 1 ปีสำหรับอุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application	1	3,540,000.00	3,540,000.00
20	MA 1 ปีสำหรับระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network)	1	798,800.00	798,800.00
21	MA 1 ปีสำหรับอุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch	1	797,600.00	797,600.00
22	MA 1 ปีสำหรับอุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง	1	462,000.00	462,000.00
23	MA 1 ปีสำหรับห้องปฏิบัติการ Security Operations Center (SOC)	1	250,000.00	250,000.00
24	SOC Services Operators 24x7 ระยะเวลา 12 เดือน	12	900,000.00	10,800,000.00
			Total (Baht)	97,996,390.00

หมายเหตุ

1. ยืนราคา : 90 วัน นับถัดจากวันที่เสนอราคา

2. ภาษีมูลค่าเพิ่ม : ราคารวมภาษีมูลค่าเพิ่มแล้ว

ด้วยความเคารพอย่างสูง

(นายเอกชัย แซ่โหง่ว)

ฝ่ายขาย

FUSION

Address : 77/148 34 Fl. Sinsathorn Tower Klongtonsai, Klongsarn, Bangkok 10600

Quotation

Quo 21-11-702

29-Oct-21

Company :	**อธิบดีกรมการปกครอง**
Project :	โครงการระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center)
Attn :	
Tel :	

We are pleased to submit you the following descriptions and the prices as follows :

Product	Description	Qty.	Per Unit Baht	Amount Baht
1	ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment) ยี่ห้อ Rapid 7 INSIGHTVM	1	1,440,600.00	1,440,600.00
2	ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor) ยี่ห้อ Riverbed รุ่น SteelCentral NetShark 4170	1	2,822,520.00	2,822,520.00
3	อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (Network access control) ยี่ห้อ Fortinet รุ่น fortinac 700C	2	2,446,085.00	4,892,170.00
4	ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) ยี่ห้อ Ninja รุ่น RMM	11,500	895.00	10,292,500.00
5	อุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) ยี่ห้อ trapx รุ่น trapx flex	2	16,366,560.00	32,733,120.00
6	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) ยี่ห้อ F5 รุ่น i11400-DA	4	5,879,580.00	23,518,320.00
7	ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (Endpoint Detection and Response) ยี่ห้อ SentinelOne รุ่น SentinelOne endpoint protection	11,500	3,528.00	40,572,000.00
8	อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway) ยี่ห้อ Trendmicro รุ่น Trendmicro DDEI 9100	2	1,255,065.00	2,510,130.00
9	ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management) ยี่ห้อ One Identity รุ่น Privileged Management	1	37,800,000.00	37,800,000.00
10	อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection) ยี่ห้อ Radware รุ่น DefensePro x420 Series	4	6,280,812.00	25,123,248.00
11	ระบบป้องกันภัยคุกคาม Domain Name System ยี่ห้อ Diamond IP รุ่น DNS Security Solutions	500	3,990.00	1,995,000.00
12	ระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร ยี่ห้อ Micro Focus รุ่น ArcSight Enterprise Security Manager	1	29,925,000.00	29,925,000.00
13	อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง ยี่ห้อ Trend Micro รุ่น Deep Discovery Inspector 4000	1	10,185,000.00	10,185,000.00
14	อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ ยี่ห้อ vectra รุ่น Cognito Platform	1	16,585,800.00	16,585,800.00
15	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย ยี่ห้อ BROADCOM รุ่น Symantec Network Forensics: Security Analytics	1	5,963,895.00	5,963,895.00
16	ลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) ยี่ห้อ Forcepoint รุ่น Forcepoint DLP	1,000	4,725.00	4,725,000.00
17	ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า Internet zone ยี่ห้อ splunk รุ่น LOG OBSERVER	2	1,869,000.00	3,738,000.00
SUB TOTAL				

FUSION

Address : 77/148 34 Fl. Sinsathorn Tower Klongtonsai, Klongsarn, Bangkok 10600

Quotation

Quo 21-11-702

29-Oct-21

Company :	อธิบดีกรมการปกครอง
Project :	โครงการระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center)
Attn :	
Tel :	

We are pleased to submit you the following descriptions and the prices as follows :

Product	Description	Qty.	Per Unit Baht	Amount Baht
18	อุปกรณ์ป้องกันเครือข่าย Internet Firewall ยี่ห้อ Check Point รุ่น 64000 Security Gateway Platform Chassis	4	30,715,185.00	122,860,740.00
19	อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application ยี่ห้อ RADWARE รุ่น ALTEON D-4208	4	9,292,500.00	37,170,000.00
20	ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network) ยี่ห้อ Palo Alto รุ่น PA-5220	2	2,815,795.00	5,631,590.00
21	อุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch ยี่ห้อ Arista รุ่น 7150S-24	4	2,093,700.00	8,374,800.00
22	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง ยี่ห้อ Arista รุ่น 7280TR-48C6	4	2,055,985.00	8,223,940.00
23	ห้องปฏิบัติการ Security Operations Center (SOC)	1	2,625,000.00	2,625,000.00
24	SOC Services Operators 24x7 (เดือน)	12	945,000.00	11,340,000.00
25	Implement Setup and Configuration สำหรับศูนย์ประมวลผลคอมพิวเตอร์คลองเก้า-นางเลิ้ง	1	9,450,000.00	9,450,000.00
SUB TOTAL				**460,498,373.00**

Payment :

รวม VAT 7% แล้ว

หมายเหตุ

กำหนดส่งมอบ : 210 วัน

ยืนราคา : 90 วัน

เงื่อนไขการชำระเงิน : 30 วัน

การรับประกัน : 1 ปี

Proposed By: **Seksan**

E-mail: Seksan@fusionsol.com

Mobile: 081 638 8257

Confirm By: ( )

Date: / / 2021

Address : 77/148 34 Fl. Sinsathorn Tower Klongtonsai, Klongsarn, Bangkok 10600

Quotation

Quo 21-11-702

29-Oct-21

Company :	อธิบดีกรมการปกครอง
Project :	ขอเสนอราคา บำรุงรักษาระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center)
Attn :	
Tel :	

We are pleased to submit you the following descriptions and the prices as follows :

Product	Description	Qty.	Per Unit Baht	Amount Baht
1	ค่า Maintenance มีถัดไป สำหรับซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment) (1 ปี)	1	648,270.00	648,270.00
2	ค่า Maintenance มีถัดไปสำหรับ ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor) (1 ปี)	1	2,822,520.00	2,822,520.00
3	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network access control) (1 ปี)	1	978,434.00	978,434.00
4	ค่า Maintenance มีถัดไปสำหรับซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) (1 ปี)	1	8,234,000.00	8,234,000.00
5	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) (1 ปี)	1	3,273,312.00	3,273,312.00
6	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) (1 ปี)	1	9,407,328.00	9,407,328.00
7	ค่า Maintenance มีถัดไปสำหรับระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response) (1 ปี)	1	12,171,600.00	12,171,600.00
8	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway) (1 ปี)	1	1,004,052.00	1,004,052.00
9	ค่า Maintenance มีถัดไปสำหรับระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management) (1 ปี)	1	6,048,000.00	6,048,000.00
10	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection) (1 ปี)	1	5,024,649.60	5,024,649.60
11	ค่า Maintenance มีถัดไปสำหรับระบบป้องกันภัยคุกคาม Domain Name System (1 ปี)	1	1,995,000.00	1,995,000.00
12	ค่า Maintenance มีถัดไปสำหรับระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM) (1 ปี)	1	3,890,250.00	3,890,250.00
13	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง (1 ปี)	1	1,018,500.00	1,018,500.00
14	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้บัญญาประดิษฐ์ (1 ปี)	1	3,317,160.00	3,317,160.00
15	ค่า Maintenance มีถัดไปสำหรับอุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย (1 ปี)	1	1,789,168.50	1,789,168.50
16	ค่า Maintenance มีถัดไปสำหรับลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) (1 ปี)	1	1,275,750.00	1,275,750.00
17	ค่า Maintenance มีถัดไปสำหรับระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone (1 ปี)	1	747,600.00	747,600.00
SUB TOTAL				

FUSION

Address : 77/148 34 Fl. Sinsathorn Tower Klongtonsai, Klongsarn, Bangkok 10600

Quotation

Quo 21-11-702

29-Oct-21

Company :	**อธิบดีกรมการปกครอง**
Project :	ขอเสนอราคา บำรุงรักษาระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center)
Attn :	
Tel :	

We are pleased to submit you the following descriptions and the prices as follows :

Product	Description	Qty.	Per Unit Baht	Amount Baht
18	ค่า Maintenance ปีถัดไปสำหรับอุปกรณ์ป้องกันเครือข่าย Internet Firewall (1 ปี)	1	31,943,792.40	31,943,792.40
19	ค่า Maintenance ปีถัดไปสำหรับอุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application (1 ปี)	1	3,717,000.00	3,717,000.00
20	ค่า Maintenance ปีถัดไปสำหรับระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network) (1 ปี)	1	1,013,686.20	1,013,686.20
21	ค่า Maintenance ปีถัดไปสำหรับอุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch (1 ปี)	1	837,480.00	837,480.00
22	ค่า Maintenance ปีถัดไปสำหรับอุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง (1 ปี)	1	822,394.00	822,394.00
23	ค่า Maintenance ปีถัดไปสำหรับห้องปฏิบัติการ Security Operations Center (SOC) (1 ปี)	1	262,500.00	262,500.00
24	SOC Services Operators 24x7 (เดือน)	12	945,000.00	11,340,000.00
SUB TOTAL				**113,582,446.70**

Payment :

รวม VAT 7% แล้ว

Proposed By: **Seksan**

E-mail: Seksan@fusionsol.com

Mobile: 081 638 8257

Confirm By: ( )

Date: / / 2021

NEXTECH ASIA CO.,LTD.

QUOTATION / ใบเสนอราคา

Project Code :

Quotation No : NTA-924/2021

Date : 28/10/2564

www.nextech-asia.com Tax ID: 0105553133087

Tel : +66 2 150 2740 Fax : +66 2 150 2741

Subject : โครงการระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center SOC)

Attn Name : อธินี กรมการปกครอง

Company : กรมการปกครอง

Item	Description	Qty.	Unit Price	Extended Price
1	ซอฟต์แวร์ประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment) (Rapid 7 INSIGHTVM)	1	1,536,640.00	1,536,640.00
2	ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor)(NetScout nGeniusONE Server)	1	3,910,655.00	3,910,655.00
3	อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC Network access control) (HPE Aruba ClearPass DL360 Appliance)	2	2,682,065.00	5,364,130.00
4	ซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) (vmware workspace one)	11,500	952.00	10,948,000.00
5	อุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution)(cybertrap cybertrap enterprise)	2	17,457,665.00	34,915,330.00
6	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)(Citrix Citrix NetScaler Application Firewall MPX 20500)	4	6,271,552.00	25,086,208.00
7	ระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR Endpoint Detection and Response) (crowdstrike Falcon Insight Endpoint Detection and Response (EDR))	11,500	3,765.00	43,297,500.00
8	อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway)(Forcepoint Forcepoint Email Security)	2	1,338,736.00	2,677,472.00
9	ระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management) (Beyondtrust Privileged Access Management)	1	38,600,000.00	38,600,000.00
10	อุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection) (NETSCOUT NETSCOUT Arbor Edge Defense (AED))	4	6,699,532.00	26,798,128.00
11	ระบบป้องกันภัยคุกคาม Domain Name System(Infoblox BloxOne Threat Defense)	500	4,256.00	2,128,000.00
12	ระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM) (LogRhythm 6350 with Direct Attached Storage 26Tb)	1	31,920,000.00	31,920,000.00
13	อุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง (Kaspersky Kaspersky Sandbox)	1	10,864,000.00	10,864,000.00
14	อุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ (fortinet fortiai)	1	17,691,520.00	17,691,520.00
15	อุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย (vmware vRealize Log Insight)	1	6,361,488.00	6,361,488.00
16	ลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention)(Broadcom Symantec Data Loss Prevention)	1000	5,040.00	5,040,000.00
17	ระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone (solarwinds SolarWinds Log & Event Manager)	2	1,993,600.00	3,987,200.00
18	อุปกรณ์ป้องกันเครือข่าย Internet Firewall (Cisco FirePOWER 8390 - security appliance)	4	29,754,140.00	119,016,560.00
19	อุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application (A10 AX 3400)	4	9,912,000.00	39,648,000.00
20	ระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network) (Check Point Quantum 6900)	2	3,342,757.00	6,685,514.00
21	อุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch (Juniper QFX5100-24Q)	4	2,106,758.00	8,427,032.00
22	อุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง (HPE FlexFabric 5945)	4	1,415,075.00	5,660,300.00
23	ห้องปฏิบัติการ Security Operations Center (SOC)	1	2,800,000.00	2,800,000.00
24	Services Operators (SOC) 24x7 ระยะเวลา 12 เดือน	12	1,008,000.00	12,096,000.00
25	Implement Setup and Configuration (ค่าลงค่า-นาเสื้อ)	1	10,080,000.00	10,080,000.00
Remark :			Amount	475,539,677.00
	Vat Included		Vat 7%	
			Total (Baht)	475,539,677.00

Terms & Condition

1 ยืนราคา 90 วัน

2 รับประกัน 1 ปี

3 เงื่อนไขการชำระเงิน 30 วัน

4 กำหนดส่งมอบ 180 วัน

We Agree & Accept to order you as in this Quotation

ข้าพเจ้าตกลงสั่งซื้อรายการตามเสนอนี้ทั้งหมด

Customer Signature with apply seal

ลงชื่อพร้อมประทับตรา

Name :

Position :

Date :

Chalisa Chairanit

Account Manager

Mobile : +668 8358 7423

Chalisa@nextech-asia.com

NEXTECH ASIA CO.,LTD

NEXTECH ASIA CO.,LTD.

QUOTATION / ใบเสนอราคา

Project Code :
Quotation No : NTA-925/2021
Date : 28/10/2564

www.nextech-asia.com
Tel : +66 2 150 2740
Tax ID: 0105553133067
Fax : +66 2 150 2741

Subject : ราคาบำรุงรักษาระบบศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยสารสนเทศ (Security Operations Center : SOC)

Attn Name : อธิบดี กรมการปกครอง

Company : กรมการปกครอง

Item	Description	Qty.	Unit Price	Extended Price
1	ค่าบำรุงรักษา 1 ปี สำหรับซอฟต์แวร์ประเมินหาความเสี่ยงที่มีช่องโหว่ด้านความปลอดภัย (Vulnerability Assessment) (MA)	1	691,488.00	691,488.00
2	ค่าบำรุงรักษา 1 ปี สำหรับซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่ายภายในองค์กร (Network performance monitor) (MA)	1	3,910,655.00	3,910,655.00
3	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network access control) (MA)	1	1,072,826.00	1,072,826.00
4	ค่าบำรุงรักษา 1 ปี สำหรับสำหรับซอฟต์แวร์ระบบป้องกันและบริหารจัดการเครื่องคอมพิวเตอร์ปลายทาง (Desktop Device Management Software) (MA)	1	8,758,400.00	8,758,400.00
5	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ป้องกันภัยคุกคามเชิงกลยุทธ์ (Deception Solution) (MA)	1	3,491,533.00	3,491,533.00
6	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) (MA)	1	10,034,483.20	10,034,483.20
7	ค่าบำรุงรักษา 1 ปี สำหรับระบบป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (EDR: Endpoint Detection and Response) (MA)	1	12,989,250.00	12,989,250.00
8	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร Email (Email security gateway) (MA)	1	1,070,988.80	1,070,988.80
9	ค่าบำรุงรักษา 1 ปี สำหรับระบบบริหารจัดการบัญชีผู้ใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Privileged Account Security Management) (MA)	1	6,176,000.00	6,176,000.00
10	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ป้องกัน DDoS ภายในและภายนอกเครือข่ายขององค์กร (DDos Protection) (MA)	1	5,359,625.60	5,359,625.60
11	ค่าบำรุงรักษา 1 ปี สำหรับระบบป้องกันภัยคุกคาม Domain Name System (MA)	1	2,128,000.00	2,128,000.00
12	ค่าบำรุงรักษา 1 ปี สำหรับระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM) (MA)	1	4,149,600.00	4,149,600.00
13	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ตรวจจับและป้องกันภัยคุกคามขั้นสูง (MA)	1	1,086,400.00	1,086,400.00
14	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์วิเคราะห์ความปลอดภัยโดยใช้ปัญญาประดิษฐ์ (MA)	1	3,538,304.00	3,538,304.00
15	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ออกรายงาน และจัดเก็บข้อมูลระบบเครือข่าย (MA)	1	1,908,446.40	1,908,446.40
16	ค่าบำรุงรักษา 1 ปี สำหรับลิขสิทธิ์การใช้งานระบบการป้องกันข้อมูลรั่วไหล (Data Loss Prevention) (MA)	1	1,360,800.00	1,360,800.00
17	ค่าบำรุงรักษา 1 ปี สำหรับระบบบริหารจัดเก็บข้อมูล Log สำหรับอุปกรณ์หน้า internet zone (MA)	1	797,440.00	797,440.00
18	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์ป้องกันเครือข่าย Internet Firewall (MA)	1	30,944,305.60	30,944,305.60
19	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์กระจายการทำงานและป้องกันการโจมตี Application (MA)	1	3,964,800.00	3,964,800.00
20	ค่าบำรุงรักษา 1 ปี สำหรับระบบเชื่อมต่อเครือข่ายเสมือนระยะไกล (Secure Sockets Layer virtual private network) (MA)	1	1,203,392.52	1,203,392.52
21	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์กระจายสัญญาณ (L3 Switch) 24-port 1/10/25G switch (MA)	1	842,703.20	842,703.20
22	ค่าบำรุงรักษา 1 ปี สำหรับอุปกรณ์กระจายสัญญาณ (L3 Switch) 10Gbps ขนาด 48 ช่อง (MA)	1	566,080.00	566,080.00
23	ค่าบำรุงรักษา 1 ปี สำหรับห้องปฏิบัติการ Security Operations Center (SOC) (MA)	1	280,000.00	280,000.00
24	Services Operators (SOC) 24x7 ระยะเวลา 12 เดือน	12	1,008,000.00	12,096,000.00

Remark :

Vat Included

Amount	118,421,471.32
Vat 7%	-
Total (Baht)	118,421,471.32

Terms & Condition

We Agree & Accept to order you as in this Quotation
ข้าพเจ้าตกลงสั่งซื้อรายการตามเงื่อนไขทั้งหมด

Customer Signature with apply seal
ลงชื่อพร้อมประทับตรา

Name :
Position :
Date :

Chalisa Chairanit
Account Manager
Mobile : +668 8358 7423
Chalisa@nextech-asia.com

NEXTECH ASIA CO.,LTD