ข้อกำหนดและขอบเขตงาน (Terms of Reference : TOR)
โครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์
และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2565

1. หลักการและเหตุผล

เนื่องจากปัจจุบัน มีภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่หลากหลายรูปแบบ เช่น Unknown Malware, Advanced Persistent Threat (APT) และ Ransomware ประเภทต่างๆ โดยในแต่ละวันจะมีการเกิดถูกโจมตีเป็นจำนวนมาก ซึ่งการนิคมอุสาหกรรมแห่งประเทศไทย (กนอ.) ได้ตระหนักถึงความสำคัญในการยกระดับการเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และเพื่อให้สอดกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยต้องมีมาตรการหรือการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงขององค์กร หรือข้อมูลส่วนบุคคลที่ทางองค์กรมีการเก็บรวบรวมไว้ ซึ่งหนึ่งในการดำเนินการหลักที่ทางองค์กรพิจารณา คือ การบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ เพื่อทำหน้าที่เฝ้าระวังและรับมือภัยคุกคามทาง ไซเบอร์ขององค์กรได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถช่วยให้องค์กรรับรู้ถึงสถานการณ์ภัยคุกคามทางไซเบอร์ต่างๆ และระบุถึงเหตุการณ์ผิดปกติได้อย่างรวดเร็วและแม่นยำ รวมทั้งตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้ทันท่วงที

จากเหตุผลที่กล่าวข้างต้นทำให้ กนอ. มีความประสงค์จะดำเนินการจ้างบริการตรวจสอบช่องโหว่ (Vulnerability Assessment: VA) และทดสอบเจาะระบบ (Penetration Testing) และใช้บริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (SOC) เพื่อทำหน้าที่เฝ้าระวังและการบริหารความเสี่ยงในการรับมือภัยคุกคามทางไซเบอร์ให้ครอบคลุม รวมทั้งความรู้ความสามารถของบุคลากร ให้สอดคล้องกับนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ของ กนอ. และโครงสร้างระบบเทคโนโลยีที่เป็นส่วนประกอบของการรักษาความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

2. วัตถุประสงค์

2.1 เพื่อดำเนินการตรวจสอบช่องโหว่ (Vulnerability Assessment: VA) ของอุปกรณ์เครือข่าย (Network Equipment) และเครื่องแม่ข่าย (Server) ของฝ่ายดิจิทัล (ฝดจ.) และศูนย์เฝ้าระวังคุณภาพสิ่งแวดล้อมและความปลอดภัย (ศสป.)

2.2 เพื่อดำเนินการทดสอบเจาะระบบ (Penetration Testing) กับระบบอนุมัติ-อนุญาตทางอิเล็กทรอนิกส์ (e-Permission & Privilege: e-PP) ของ กนอ.

2.3 เพื่อยกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานสากล โดยการเฝ้าระวังและรับมือกับภัยคุกคามด้านไซเบอร์ ตลอด 24 ชั่วโมง ซึ่งสอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.4 เพื่อสร้างความตระหนักให้กับเจ้าหน้าที่ของ กนอ. ให้มีความพร้อมสำหรับการรับมือต่อภัยคุกคามทางไซเบอร์

3. คุณสมบัติผู้ยื่นข้อเสนอ

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 ผู้ยื่นข้อเสนอต้องเป็นนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ กนอ. ณ วันยื่นข้อเสนอ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการเสนอราคาครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

3.11 ผู้ยื่นข้อเสนอต้องได้รับรองมาตรฐาน ISO/IEC 27001:2013 สำหรับศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operations Center: SOC ซึ่งตั้งอยู่ในประเทศไทย โดยมีเจ้าหน้าที่ประจำปฏิบัติงานในศูนย์ฯ ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7) ทั้งนี้ เจ้าหน้าที่ประจำปฏิบัติงานในศูนย์ฯ จะต้องเป็นพนักงานประจำของผู้รับจ้าง และไม่ใช่การจ้างพนักงานแบบชั่วคราว (Outsource)

3.12 ผู้ยื่นข้อเสนอต้องมีผลงานในการให้บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยให้บริการตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7) หรือให้บริการสอดคล้องกับขอบเขตงาน ซึ่งเป็นผลงานที่แล้วเสร็จไม่เกิน 5 ปี นับถึงวันยื่นข้อเสนอ และเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ รัฐวิสาหกิจหรือหน่วยงานเอกชนที่ กนอ. เชื่อถือ อย่างน้อย 1 โครงการ ซึ่งมูลค่าของโครงการไม่น้อยกว่า 3,000,000 บาท (สามล้านบาทถ้วน) ทั้งนี้ ผู้ยื่นข้อเสนอต้องแสดงหนังสือรับรองผลงานหรือสำเนาสัญญาฯ พร้อมกับการยื่นข้อเสนอด้วย

4. ขอบเขตการดำเนินงาน

4.1 จัดทำแผนการดำเนินงานตลอดระยะเวลาของโครงการ และส่งมอบให้แก่ กนอ. ภายใน 15 วัน นับถัดจากวันที่ลงนามในสัญญา โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

4.1.1 ประเมินความเสี่ยง/ผลกระทบที่อาจเกิดขึ้นจากการดำเนินการตรวจสอบช่องโหว่ (VA) และทดสอบเจาะระบบ (Penetration Testing)

4.1.2 กำหนดเป้าหมายของอุปกรณ์ที่จะตรวจสอบช่องโหว่ (VA) จำนวนไม่น้อยกว่า 80 IP Address

4.1.3 จัดทำแผนการดำเนินงานโดยระบุ วัน เวลา สถานที่และบุคลากรที่ดำเนินการตรวจสอบช่องโหว่และทดสอบเจาะระบบ โดยบุคลากรที่เป็นผู้รับผิดชอบจะต้องดำเนินการด้วยตนเองตลอดระยะเวลาตามแผนการดำเนินงาน

4.1.4 แผนผังของบุคลากรและช่องทางการติดต่อสื่อสารของผู้รับจ้าง

4.1.5 รายละเอียดของซอฟต์แวร์สำหรับการตรวจสอบช่องโหว่และทดสอบเจาะระบบ

4.1.6 แผนการติดตั้งอุปกรณ์จัดเก็บข้อมูล Log จากเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย เข้าสู่ระบบวิเคราะห์ข้อมูลระบบ SIEM ของผู้รับจ้าง

4.1.7 แผนการติดตั้งระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Endpoint Detection and Response : EDR)

4.2 ดำเนินการตรวจสอบช่องโหว่ (VA) โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

4.2.1 ตรวจสอบช่องโหว่ (VA) ครั้งที่ 1 ของอุปกรณ์เครือข่าย (Network Equipment) และเครื่องแม่ข่าย (Server) ของ กนอ. จำนวนไม่น้อยกว่า 80 IP Address โดยใช้โปรแกรมประเภทมีลิขสิทธิ์ 1 โปรแกรม และ Open Source หรือ Freeware 1 โปรแกรม

4.2.2 วิเคราะห์ และจัดลำดับความเสี่ยง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการตรวจสอบช่องโหว่ (VA) ครั้งที่ 1

4.2.3 ร่วมดำเนินการกับผู้ดูแลระบบของ กนอ. เพื่อปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ครั้งที่ 1 ซึ่งเป็นช่องโหว่ที่สามารถดำเนินการแก้ไขได้โดยไม่ต้องจัดซื้อโปรแกรมที่มีลิขสิทธิ์ หรือไม่ต้องจัดหาอุปกรณ์ป้องกันเพิ่มเติม และไม่กระทบกับระบบงานของ กนอ. ตามขอบเขตของงานและระยะเวลาการดำเนินการที่ กนอ. เห็นชอบ และจัดทำรายงานผลการปิดช่องโหว่ครั้งที่ 1 โดยนำเสนอต่อ กนอ. อย่างละเอียด

4.2.4 ตรวจสอบช่องโหว่ (VA) ครั้งที่ 2 ของอุปกรณ์เครือข่าย (Network Equipment) และเครื่องแม่ข่าย (Server) ของ กนอ. จำนวนไม่น้อยกว่า 80 IP Address ซึ่งมีรายการอุปกรณ์ไม่น้อยกว่าการตรวจสอบช่องโหว่ในครั้งที่ 1 โดยใช้โปรแกรมประเภทมีลิขสิทธิ์ 1 โปรแกรม และ Open Source หรือ Freeware 1 โปรแกรม

4.2.5 วิเคราะห์ และจัดลำดับความเสี่ยง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการตรวจสอบช่องโหว่ (VA) ครั้งที่ 2

4.3 ดำเนินการทดสอบเจาะระบบ (Penetration Testing) โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

4.3.1 ทดสอบเจาะระบบอนุมัติ-อนุญาตทางอิเล็กทรอนิกส์ (e-PP) ครั้งที่ 1 ในรูปแบบ Grey-Box จำนวน 2 Roles

4.3.2 วิเคราะห์ และจัดลำดับความเสี่ยง โดยอ้างอิงตาม OWASP Top 10 เวอร์ชั่นล่าสุด หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการทดสอบเจาะระบบ e-PP (Penetration Testing) ครั้งที่ 1

4.3.3 ทดสอบเจาะระบบอนุมัติ-อนุญาตทางอิเล็กทรอนิกส์ (e-PP) ครั้งที่ 2 ในรูปแบบ Grey-Box จำนวน 2 Roles

4.3.4 วิเคราะห์ และจัดลำดับความเสี่ยง โดยอ้างอิงตาม OWASP Top 10 เวอร์ชั่นล่าสุด หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง และจัดทำข้อเสนอแนะแนวทางการปิดช่องโหว่ที่ตรวจพบ จากการทดสอบเจาะระบบ e-PP (Penetration Testing) ครั้งที่ 2

4.4 บริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operation Center : SOC)

ผู้รับจ้างจะต้องมีบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7) เพื่อให้ กนอ. ได้รับการแจ้งเตือนภัยคุกคามทางไซเบอร์และวิธีการตรวจสอบและแก้ไขได้อย่างถูกต้อง มีประสิทธิภาพ โดยมีคุณลักษณะดังต่อไปนี้

4.4.1 ต้องจัดให้มีระบบรวบรวมข้อมูลจราจรทางคอมพิวเตอร์ (Log File) จากเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย เข้าสู่ระบบวิเคราะห์ข้อมูลระบบ SIEM ของผู้รับจ้าง ตามรายการอุปกรณ์อย่างน้อยดังนี้

4.4.1.1 สำหรับ กนอ.สนญ หรือ สนพ. หรือ สทร. (จังหวัดระยอง)

- Firewall จำนวน 1 เครื่อง
- Active Directory จำนวน 2 เครื่อง
- Antivirus Gateway จำนวน 1 เครื่อง
- Virtualization Host จำนวน 6 เครื่อง
- ERP Application Server จำนวน 1 เครื่อง
- ERP Database Server จำนวน 1 เครื่อง
- Workflow Server จำนวน 2 เครื่อง
- Intranet Server จำนวน 2 เครื่อง
- SDWAN Analysis จำนวน 1 ระบบ

4.4.1.2 สำหรับ ศสป.

- Active Directory จำนวน 1 เครื่อง
- DSS Server จำนวน 1 เครื่อง
- E-Monitoring Server จำนวน 1 เครื่อง
- Envista Server จำนวน 1 เครื่อง
- Emergency Online Server จำนวน 1 เครื่อง
- SDWAN Analysis จำนวน 1 ระบบ

4.4.2 ผู้รับจ้างต้องดำเนินการร่วมกับเจ้าหน้าที่ กนอ. ในการตั้งค่าตามรายการอุปกรณ์ที่ใช้งานอยู่ในปัจจุบัน เพื่อให้มีการส่งข้อมูลจราจรทางคอมพิวเตอร์ (Log file) จากเครื่องและอุปกรณ์ดังกล่าวไปยังอุปกรณ์จัดเก็บข้อมูล Log ของผู้รับจ้าง

4.4.3 ผู้รับจ้างต้องติดตั้งอุปกรณ์หรือซอฟแวร์ในการจัดเก็บข้อมูล Log (Log Collector, Event Collector) ที่ กนอ.สนญ. หรือ สนพ. หรือ สทร. และ ศสป. ตามความเหมาะสม เพื่อจัดเก็บข้อมูล Log ส่งไปยังศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ของผู้รับจ้าง โดย กนอ. จะเป็นผู้จัดเตรียมช่องทางสื่อสาร (Internet Link) สำหรับการส่งข้อมูลดังกล่าว

4.4.4 ต้องสามารถวิเคราะห์เหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต เพื่อวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring) แหล่งที่มาของภัยคุกคามนั้นๆ ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7)

4.4.5 ผู้รับจ้างต้องทำการเฝ้าระวัง วิเคราะห์ และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ ผ่านทาง E-mail, โทรศัพท์ และระบบ Ticket Management ตาม Service Level Agreement และระดับความรุนแรงที่ กนอ. กำหนดดังต่อไปนี้

ระดับความรุนแรง	ผลกระทบ	เวลาในการแจ้งเตือนแก่ กนอ.	ให้คำแนะนำในการแก้ไข
สูง (High)	การดำเนินธุรกิจหยุดชะงัก และจำเป็นต้องแก้ไขอย่างเร่งด่วนที่สุด	ภายใน 30 นาที	ภายใน 60 นาที
ปานกลาง (Medium)	ผลกระทบต่อการดำเนินธุรกิจ และมีความจำเป็นต้องแก้ไขอย่างทันท่วงที	ภายใน 60 นาที	ภายใน 120 นาที
ต่ำ (Low)	ผลกระทบต่อประสิทธิภาพการทำงานทั่วไป และมีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวมเล็กน้อย	ภายใน 90 นาที	ภายใน 180 นาที
ต่ำมาก (Very Low)	ผลกระทบต่อประสิทธิภาพการทำงานทั่วไป และไม่มีผลกระทบต่อการดำเนินธุรกิจโดยภาพรวม	ข้อมูลรายงาน	ข้อมูลรายงาน

4.4.6 การแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ต้องครอบคลุมเนื้อหาดังต่อไปนี้

- ระบุประเภทของภัยคุกคาม
- วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม
- ระบุต้นทาง (Attacker) และปลายทาง (Target)
- ระบุระดับความรุนแรง (Severity)
- ภาพการเชื่อมโยงเหตุการณ์ภัยคุกคามที่เกิดขึ้น
- รายละเอียดเหตุการณ์และพฤติกรรมทั้งหมด
- คำแนะนำและขั้นตอนการดำเนินการแก้ไขเชิงเทคนิค

4.4.7 ผู้รับจ้างต้องมีระบบบริหารจัดการ ซึ่งแสดงสถานการณ์ตรวจสอบข้อมูลความปลอดภัยของระบบเครือข่าย และข้อมูลการแจ้งเตือนและติดตามเหตุการณ์ (Ticket Management) เพื่อให้ กนอ. สามารถตรวจสอบข้อมูลได้ตลอดเวลา

4.4.8 ผู้รับจ้างต้องจัดให้มีทีมงานผู้เชี่ยวชาญ เพื่อเข้าดำเนินการสืบสวนและวิเคราะห์หาสาเหตุของปัญหาภัยคุกคามที่เกิดขึ้นในความรุนแรงระดับสูงมาก (Very High) ณ สถานที่ที่เกิดเหตุภัยคุกคามทางไซเบอร์ รวมทั้งให้คำแนะนำแนวทางการแก้ไขและป้องกันปัญหาตามที่ กนอ. ร้องขอ ไม่เกินกว่า 12 ครั้งต่อปี

4.4.9 ผู้รับจ้างต้องดำเนินการจัดทำรายงานสรุปผลการเฝ้าระวังภัยคุกคามแบบรายเดือน (Monthly Report) และรายงานข่าวสารที่เกี่ยวกับคุกคามใหม่ที่เกิดขึ้นด้านความปลอดภัยไซเบอร์ที่เกิดขึ้นทั่วโลก ให้แก่ กนอ. แบบรายเดือน พร้อมนัดประชุมกับ กนอ. เพื่อสรุปภาพรวมผลการเฝ้าระวังภัยคุกคามและภัยคุกคามใหม่ ที่เกิดขึ้นและให้คำปรึกษาในการรับมือกับภัยคุกคามที่เกิดขึ้นให้ทางเจ้าหน้าที่ กนอ.

4.4.10 ผู้รับจ้างต้องดำเนินการจัดทำรายงานผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ และสรุปผลการดำเนินการเฝ้าระวังภัยคุกคามเหตุการณ์ผิดปกติที่เป็นภัยคุกคามเป็นรายเดือน (Monthly report) โดยมีรายละเอียดดังต่อไปนี้

4.4.10.1 รายงานสรุปสำหรับผู้บริหาร (Executive Summary) เพื่ออธิบายผู้บริหารให้เข้าใจสถานะความเสี่ยงและสภาพปัจจุบัน

4.4.10.2 รายงานสรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้นโดยมีการวิเคราะห์ภัยคุกคามในเชิงลึก โดยมีเนื้อหาตามรายการดังต่อไปนี้เป็นอย่างน้อย

- Top Attackers Report
- Top Threat Report
- รายงานสรุปปริมาณการใช้งานข้อมูลจราจรทางคอมพิวเตอร์ประจำเดือน
- รายงานสรุปการแจ้งเตือนเหตุการณ์ที่ตรวจพบ (Incident Report) ประจำเดือน

4.4.11 ต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบและมาตรฐานของผู้รับจ้าง อ้างอิง มาตรฐาน NIST Incident Categories เป็นอย่างน้อย

4.4.12 บริการเฝ้าระวังและแจ้งเตือนภัยคุกคามด้วยรูปแบบเงื่อนไขเฉพาะ หรือเงื่อนไขอื่นๆ เพิ่มเติมให้เหมาะสม (Custom Use case) ตามที่ กนอ. กำหนด จำนวนไม่เกิน 10 Custom Use case

4.4.13 ต้องมี Rules ที่ใช้กับอุปกรณ์เฝ้าระวัง สามารถตรวจจับเหตุการณ์การคุกคามซึ่งครอบคลุมในเรื่องดังนี้เป็นอย่างน้อย

1) Unauthorized Access

2) Malicious Code

3) Inappropriate Usage

4) Multiple Component

5) Denial of Service (DOS)

6) Exercise/Network Defense Testing

4.4.14 บริการแจ้งข่าวสารซึ่งเกี่ยวข้องกับระบบรักษาความปลอดภัยทางไซเบอร์ ระบบคอมพิวเตอร์และระบบเครือข่าย ผ่านทางอีเมล์ (News Letter) และแอพพลิเคชั่นไลน์ เช่น

1) รายชื่อ และคุณลักษณะของมัลแวร์ (Malware)

2) ช่องโหว่ใหม่ (Vulnerability) ของอุปกรณ์ในระบบเครือข่าย (Network Equipment)

3) ช่องโหว่ใหม่ (Vulnerability) ของระบบปฏิบัติการ (Operating System)

4) ช่องโหว่ใหม่ (Vulnerability) ของระบบฐานข้อมูลหลัก (Database)

5) ช่องโหว่ใหม่ (Vulnerability) ของโปรแกรมที่ผู้รับจ้างเห็นว่าจะก่อให้เกิดผลเสียหายต่อการดำเนินงานของ กนอ.

โดยข่าวสารดังกล่าวต้องประกอบด้วยเนื้อหาที่สำคัญอย่างน้อยดังต่อไปนี้ 1) คำอธิบายทั่วไป (Overview) 2) คำอธิบายอย่างละเอียด (Description) 3) ผลกระทบ (Impact) 4) ระบบที่ได้รับผลกระทบ (System Affected) 5) การแก้ไข (Solution) (ถ้ามี) และ 6) การอ้างอิง (Reference)

4.4.15 บริการค้นหาภัยคุกคามเชิงรุก (Threat Hunting) หรือดำเนินการค้นหารูปแบบการโจมตีจาก Threat Intelligence โดยใช้เครื่องมือของผู้รับจ้าง และแจ้งเตือนให้ทราบถึงภัยคุกคามที่จะเกิดขึ้นกับ กนอ.

4.4.16 บริการแก้ไขปัญหา และจัดทำรายงานสรุปการแก้ไขปัญหาที่ได้รับแจ้งจากศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (SOC) ของผู้รับจ้าง โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้ 1) วัน เดือน ปี ที่รับแจ้ง 2) เวลารับแจ้ง 3) ปัญหาที่ได้รับแจ้ง 4) รายงานการแก้ไขปัญหา 5) สถานะในการดำเนินการ

4.4.17 บริการประเมินความเสี่ยงด้านไซเบอร์ (Security Risk Rating) และจัดทำรายงานสรุปพร้อมแนวทางการแก้ไขปัญหา โดยจัดทำการประเมินจำนวน 4 ครั้งต่อปี

4.4.18 บริการจำลองช่องโหว่และการโจมตีเพื่อการทดสอบประสิทธิภาพการป้องกันและตรวจจับภัยคุกคามทางไซเบอร์ภายใต้การควบคุม พร้อมคำแนะนำในการแก้ไขอุปกรณ์เพื่อปิดกั้นช่องโหว่ จำนวน 1 ครั้งต่อปี

4.5 บริการจำลองอีเมลฟิชชิงด้วยรูปแบบเหตุการณ์เสมือนจริง (Phishing Simulation)

ผู้รับจ้างจะต้องจัดให้มีการทดสอบจำลองอีเมลฟิชชิงด้วยรูปแบบเหตุการณ์เสมือนจำนวนไม่น้อยกว่า 600 User อย่างน้อย 2 ครั้ง เพื่อสร้างประสบการณ์และความคุ้นเคยต่อรูปแบบของอีเมลฟิชชิงให้กับบุคลากรของ กนอ. รวมถึงฝึกฝนเทคนิควิธีในการสังเกตและแยกแยะอีเมลฟิชชิง โดยระบบจำลองอีเมลฟิชชิงด้วยรูปแบบเหตุการณ์เสมือนจริง และจัดทำรายงานผลการทดสอบ

4.6 บริการระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Endpoint Detection and Response : EDR) จำนวนไม่น้อยกว่า 600 User โดยมีคุณลักษณะอย่างน้อยดังนี้

ผู้รับจ้างจะต้องเสนอระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย โดยมีเทคโนโลยี แบบที่ 1 (ข้อกำหนด 4.6.1) หรือ แบบที่ 2 (ข้อกำหนด 4.6.2) อย่างใดอย่างหนึ่ง ดังนี้

4.6.1 ระบบ EDR แบบที่ 1

1) สามารถติดตั้งร่วมกับระบบปฏิบัติการ (Operating Systems) ดังนี้ Windows 11, Windows 10, Windows 8.1, Windows 8 และ Windows 7

2) รองรับการติดตั้งโปรแกรมผ่านโปรแกรมบริหารจัดการจากส่วนกลาง (Network Discovery) หรือแบบส่งเป็น e-mail หรือ ติดตั้งเอง โดยใช้ไฟล์ติดตั้งด้วยไฟล์เดียวได้

3) สามารถทำการตรวจจับ Malware ประเภทดังต่อไปนี้ได้ ไวรัส, โทรจัน, Worm, Rootkit, Phishing, Adware, Keylogger เป็นอย่างน้อย

4) มีฟังก์ชันในการเฝ้าระวังการทำงานของ Ransomware เพื่อป้องกันไม่ให้สร้างความเสียหายกับเครื่องแม่ข่ายและเครื่องลูกข่ายได้ (Ransomware Vaccine หรือ Ransomware Mitigation หรือ Ransomware Protection) โดยสามารถกู้คืนไฟล์ที่ถูกเข้ารหัสได้อัตโนมัติ

5) สามารถกำหนดนโยบายการรักษาความปลอดภัย เพื่อนำไปใช้โดยผู้ใช้ปลายทางไม่สามารถยกเลิกหรือแก้ไขนโยบายได้เอง

6) สามารถสั่งสแกน/อัพเดตทันทีหรือกำหนดช่วงเวลาการ สแกน/อัพเดต ได้จาก Management Console

7) ผู้ดูแลระบบ สามารถเลือกที่จะทำการลบไฟล์ (Delete) ที่ต้องสงสัยว่าเป็นไวรัส หรือสามารถกักกันไฟล์ (Quarantine) ที่ต้องสงสัยได้

8) ต้องสามารถกำหนดพาสเวิร์ดในการป้องกันการรถอนการติดตั้งโปรแกรมได้

9) สามารถอัพเดตฐานข้อมูล Malware ผ่านทาง Web Management Console ได้หรืออัพเดตผ่านทางเครื่องแม่ข่ายและเครื่องลูกข่ายที่อยู่ในระบบเครือข่ายเดียวกันได้ โดยสามารถเลือกกำหนด ได้เพียงช่องทางเดียวหรือได้ทั้งสองช่องทาง

10) สามารถกำหนดให้เครื่องแม่ข่ายและเครื่องลูกข่ายทำหน้าที่รับข้อมูลการอัพเดตจากทาง Management Console และเครื่องดังกล่าวสามารถกระจายข้อมูลการ Update ต่อไปยังเครื่องลูกข่ายอื่นๆได้

11) เมื่อตรวจพบ Malware สามารถทำการแจ้งเตือนไปยังผู้ดูแลระบบผ่านทางอีเมลได้ โดยอัตโนมัติ โดยสามารถกำหนดให้ส่งได้อย่างน้อย 1 อีเมล

12) สามารถทำการคืนไฟล์ (Restore) ที่ถูกกักกัน (Quarantine) กลับไปยังตำแหน่งเดิมได้โดยผ่านทาง Management Console หรือผ่านทางเครื่องลูกข่าย หรือกำหนด โฟลเดอร์ปลายทางที่ต้องการใหม่ได้

13) สามารถกำหนดการอัพเดต ได้ตามช่วงเวลาโดยแบ่งตามกลุ่ม เพื่อสามารถจัดสรรการอัพเดตได้

14) สามารถกำหนดการเข้าถึงเว็บไซต์หรือ โปรแกรม ว่าอนุญาต/ไม่อนุญาต ให้เข้าใช้งานได้

15) สามารถ Block เว็บไซต์หลอกลวงหรือเว็บไซต์ที่อาจเป็นอันตรายได้ (Anti-Phishing)

16) มีหรือสามารถควบคุมไฟล์วอลที่สามารถป้องกันภัยคุกคามที่เข้ามาโจมตีได้

17) สามารถตรวจจับแอนตี้ไวรัสที่ใช้งานอยู่ก่อนการติดตั้งใหม่ ได้ไม่น้อยกว่า 10 ชนิด เพื่อการถอดถอนแอนตี้ไวรัสหรือสามารถทำงานร่วมกัน ก่อนการติดตั้ง

18) สามารถทำการสแกนอุปกรณ์จัดเก็บข้อมูล (Removable Drive) และ Network drive ได้

19) มีเทคโนโลยีการสแกนอย่างน้อยดังต่อไปนี้

19.1) Local scan: การสแกนโดยใช้ทรัพยากรที่มีอยู่ในเครื่องเครื่องแม่ข่ายและเครื่องลูกข่าย เท่านั้น

19.2) Hybrid scan หรือ Live Protection: การสแกนโดยใช้ทรัพยากรเพียงส่วนหนึ่งในเครื่องแม่ข่ายและเครื่องลูกข่ายและใช้ Cloud security ในการช่วยสแกน

19.3) Central scan หรือ Sample Submission หรือ Request latest intelligence: การสแกนโดยส่งไฟล์ต้องสงสัยไปสแกนยังระบบส่วนกลางของทางระบบป้องกันไวรัส

20) มีเทคโนโลยีตรวจสอบไฟล์เพื่อไม่ทำการสแกนซ้ำไฟล์เดิม แต่จะทำการสแกนไฟล์ที่เป็นไฟล์ใหม่และไฟล์ที่มีการอัพเดตหรือไฟล์ติดไวรัส

21) สามารถอนุญาต/ไม่อนุญาตให้ใช้งานหรือไม่ให้ใช้งานอุปกรณ์ต่อพ่วงจำพวก External storage, Internal storage, Bluetooth, Network adaptor, Imaging device ได้

22) มีเทคโนโลยีการป้องกันการโจมตีประเภท Fileless attacks และ Script-based attacks ได้

23) มีเทคโนโลยีสำหรับการตรวจสอบไฟล์ ก่อนทำการ Run File (Pre Execution Stage) ดังนี้

23.1) Targeted Attack

23.2) Suspicious files and network traffic

23.3) Exploits

23.4) Ransomware

23.5) Grayware

24) มีเทคโนโลยี Sandbox Analyzer หรือ Threat Intelligence สำหรับการตรวจสอบวิเคราะห์พฤติกรรมของไฟล์ที่ต้องสงสัยแบบอัตโนมัติ และแบบส่งไฟล์ไปวิเคราะห์บน Cloud ได้ด้วยตนเอง

25) มีเทคโนโลยีการทำงาน EDR แบบ Cloud เพื่อทำงานร่วมกับระบบป้องกันไวรัสหรือ EPP (Endpoint Protection Platform) ได้

26) มีการแสดงผล Incidents ที่แสดง Timeline และ Events Record เพื่อดูกิจกรรมที่ต้องสงสัยในแบบเรียลไทม์ พร้อมทั้งหลักฐานที่ได้ทำการวิเคราะห์ ด้วยเทคโนโลยีแบบ Threat Analysis

27) มีความสามารถในการทำ Locally monitors processes ในเครื่องคอมพิวเตอร์ และ Remote monitors network share เกี่ยวกับการทำงานของ Ransomware และสามารถทำการกู้คืนไฟล์ (Recover) ที่ถูก Ransomware เมื่อมีการตรวจพบแบบ Automatically

4.6.2 ระบบ EDR แบบที่ 2 ต้องมีคุณสมบัติเทียบเท่า หรือดีกว่า แบบที่ 1 โดยต้องครอบคลุมการป้องกัน เฝ้าระวัง และตอบสนอง ให้สอดคล้องกับระบบที่เกี่ยวข้องทั้งหมดของ กนอ. ในปัจจุบัน

4.6.3 ผู้รับจ้างต้องบริหารและจัดการระบบ EDR ให้กับ กนอ. ดังต่อไปนี้

4.6.3.1 ประสานงาน และดำเนินการร่วมเจ้าหน้าที่กนอ. ในการติดตั้งระบบ EDR โดยต้องดำเนินการตามแผนงานและวิธีการที่ กนอ. เห็นชอบก่อนการติดตั้ง

4.6.3.2 มีเจ้าหน้าที่ ให้คำปรึกษาและแก้ไขปัญหาตลอด 24 ชั่วโมง ผ่านช่องทาง Email และโทรศัพท์

4.6.3.3 ให้คำปรึกษา แนะนำเกี่ยวกับการใช้งานระบบ EDR แก่เจ้าหน้าที่ กนอ.

4.6.3.4 ออกแบบสถาปัตยกรรมการเชื่อมต่อ และการทำงานร่วมกับระบบที่เกี่ยวข้องทั้งหมดของ กนอ. และระบบของบริการที่ผู้รับจ้างนำเสนอ ครอบคลุมการป้องกัน เฝ้าระวัง และตอบสนอง ให้สอดคล้องกับระบบของ กนอ. พร้อมทั้งยืนยันว่าไม่กระทบกับระบบปัจจุบันของ กนอ และในกรณีที่มีผลกระทบต้องรับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

4.7 บริการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (Managed Detection and Response: MDR) จำนวนไม่น้อยกว่า 600 User โดยมีคุณลักษณะอย่างน้อยดังนี้

4.7.1 บริการ Threat Response Managed Service โดยเจ้าหน้าที่ผู้เชี่ยวชาญภายใต้เครื่องหมายการค้าเดียวกันกับ EDR ตลอด 24 ชั่วโมง ต่อวัน 7 วันต่อสัปดาห์ (24/7) ผ่านหน้าบริหารจัดการกลางเดียวกันกับ Endpoint Protection และ Endpoint Detection and Response

4.7.2 ต้องมีเจ้าหน้าที่ให้การสนับสนุนและตอบสนองต่อภัยคุกคามทางไซเบอร์กับทีมงานของเจ้าของผลิตภัณฑ์ตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์ (24/7)

4.7.3 ตรวจสอบ Endpoint และ EDR ให้สามารถทำงานได้อย่างเต็มประสิทธิภาพอย่างสม่ำเสมอ พร้อมทั้งแนะนำการปรับปรุงการตั้งค่าที่เหมาะสม

4.7.4 ตรวจสอบและวิเคราะห์สัญญาณอันตราย เช่น IoA และ IoC อย่างสม่ำเสมอ

5. การฝึกอบรม

5.1 ผู้รับจ้างต้องจัดให้มีการฝึกอบรมและแนะนำการใช้งานระบบ EDR ระยะเวลาไม่เกิน 6 ชั่วโมง สำหรับผู้ดูแลระบบ (Administrator) โดยรองรับผู้เข้ารับการอบรมจำนวน ไม่น้อยกว่า 10 คน พร้อมจัดส่งคู่มือการใช้งาน

5.2 ผู้รับจ้างต้องจัดให้มีการฝึกอบรมภายในประเทศพร้อมสอบใบรับรองความสามารถหลักสูตรประกาศนียบัตรผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ CompTIA : A+ หรือหลักสูตรตามที่ กนอ. เห็นชอบ จากหน่วยงานเจ้าของมาตรฐานหรือตัวแทนที่ได้รับการแต่งตั้ง จำนวน 2 คน

5.3 ผู้รับจ้างต้องจัดให้มีการฝึกอบรมภายในประเทศพร้อมสอบใบรับรองความสามารถหลักสูตรประกาศนียบัตรผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ CompTIA : Security+ หรือหลักสูตรตามที่ กนอ. เห็นชอบ จากหน่วยงานเจ้าของมาตรฐานหรือตัวแทนที่ได้รับการแต่งตั้ง จำนวน 2 คน

5.4 ผู้รับจ้างต้องจัดให้มีการฝึกอบรมภายในประเทศพร้อมสอบใบรับรองความสามารถหลักสูตรประกาศนียบัตรผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ CompTIA : CySA+ หรือหลักสูตรตามที่ กนอ. เห็นชอบ จากหน่วยงานเจ้าของมาตรฐานหรือตัวแทนที่ได้รับการแต่งตั้ง จำนวน 2 คน

ทั้งนี้ ผู้รับจ้างเป็นผู้รับผิดชอบค่าใช้จ่ายเกี่ยวกับเอกสารประกอบการฝึกอบรม อาหารและอาหารว่าง เป็นต้น เพื่อรับรองการฝึกอบรมทั้งหมด

6. การติดตั้ง

6.1 ผู้รับจ้างต้องติดตั้งอุปกรณ์จัดเก็บข้อมูล Log เพื่อดำเนินการเก็บข้อมูล Log จากอุปกรณ์รักษาความปลอดภัยและระบบอื่นๆ ของ กนอ. ตามข้อกำหนดและขอบเขตของงานข้อที่ 4.4.1 เข้าสู่ระบบวิเคราะห์ข้อมูลผ่านระบบ SIEM ของผู้รับจ้าง เพื่อเป็นประโยชน์ต่อการวิเคราะห์ภัยคุกคามทางไซเบอร์ โดยผู้รับจ้างจะต้องดำเนินการติดตั้งอุปกรณ์จัดเก็บข้อมูล Log ให้แล้วเสร็จภายในระยะเวลา 60 วัน นับถัดจากวันที่ลงนามในสัญญา

6.2 ผู้รับจ้างต้องติดตั้ง ระบบตรวจจับและตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (EDR) ตามข้อกำหนดและขอบเขตของงานข้อที่ 4.6 ภายในระยะเวลา 60 วัน นับถัดจากวันที่ลงนามในสัญญา

6.3 ผู้รับจ้างต้องติดตั้ง ตั้งค่าระบบงาน โปรแกรม และเครื่องมือทั้งหมดที่เกี่ยวข้องกับการรับจ้างตามข้อกำหนดและขอบเขตของงานนี้ให้เป็นที่เรียบร้อย และสามารถใช้งานได้อย่างถูกต้อง พร้อมนำส่งรายงานผลการดำเนินงานต่อ กนอ.

7. ระยะเวลาการส่งมอบงานและการให้บริการ

ผู้รับจ้างต้องส่งมอบงานและให้บริการแก่ กนอ. ตามเงื่อนไขและเวลาที่กำหนดไว้ ทั้งนี้ กนอ. จะชำระเงินตามสัญญาหลังจากผู้รับจ้างปฏิบัติครบถ้วนและถูกต้องตามสัญญา และผ่านการตรวจรับจากคณะกรรมการตรวจรับพัสดุฯ โดยมีรายละเอียดดังนี้

7.1 ระยะเวลาภายใน 15 วัน นับถัดจากวันลงนามในสัญญา จะต้องส่งมอบแผนการดำเนินงานตลอดระยะเวลาของโครงการตามข้อ 4.1

7.2 ระยะเวลาภายใน 45 วัน นับถัดจากวันลงนามในสัญญา

7.2.1 รายงานผลการตรวจสอบช่องโหว่ (VA) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 1 ตามข้อ 4.2.1 และ 4.2.2

7.2.1 รายงานผลการทดสอบเจาะระบบ (Penetration Testing) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 1 ตามข้อ 4.3.1 และ 4.3.2

7.3 ระยะเวลาภายใน 60 วัน นับถัดจากวันลงนามในสัญญา

7.3.1 รายงานผลการปิดช่องโหว่ตามผลการตรวจสอบช่องโหว่ (VA) ครั้งที่ 1 ตามข้อ 4.2.3

7.3.2 รายงานผลการติดตั้งอุปกรณ์จัดเก็บข้อมูล Log และรายงานผลการตั้งค่าระบบวิเคราะห์และจัดการข้อมูลจราจรด้านความปลอดภัยสำหรับให้บริการเฝ้าระวังภัยคุกคามแก่ กนอ. ตามข้อ 4.4.1

7.3.3 รายงานผลการทดสอบจำลองอีเมลฟิชชิงด้วยรูปแบบเหตุการณ์เสมือน ครั้งที่ 1 ตามข้อ 4.5

7.3.4 ส่งมอบ License ระบบ EDR ตามข้อ 4.6

7.4 ระยะเวลาภายใน 150 วัน นับถัดจากวันลงนามในสัญญา

7.4.1 รายงานผลการตรวจสอบช่องโหว่ (VA) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 2 ตามข้อ 4.2.4 และ 4.2.5

7.4.2 รายงานผลการทดสอบเจาะระบบ (Penetration Testing) พร้อมการวิเคราะห์และจัดทำข้อเสนอแนะ ครั้งที่ 2 ตามข้อ 4.3.3 และ 4.3.4

7.4.3 รายงานผลการทดสอบจำลองอีเมลฟิชชิงด้วยรูปแบบเหตุการณ์เสมือน ครั้งที่ 2 ตามข้อ 4.5

7.4.4 รายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามข้อ 4.4.9

7.4.5 รายงานประจำเดือน สรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ 4.4.10

7.4.6 รายงานประจำเดือน สรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามข้อ 4.7

7.5 ระยะเวลาภายใน 240 วัน นับถัดจากวันลงนามในสัญญา

7.5.1 รายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามข้อ 4.4.9

7.5.2 รายงานประจำเดือน สรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ 4.4.10

7.5.3 รายงานประจำเดือน สรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามข้อ 4.7

7.6 ระยะเวลาภายใน 330 วัน นับถัดจากวันลงนามในสัญญา

7.6.1 รายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามข้อ 4.4.9

7.6.2 รายงานประจำเดือน สรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ 4.4.10

7.6.3 รายงานประจำเดือน สรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามข้อ 4.7

7.7 ระยะเวลาภายใน 420 วัน นับถัดจากวันลงนามในสัญญา

7.7.1 รายงานประจำเดือน สรุปผลการเฝ้าระวังภัยคุกคามด้วยศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ตามข้อ 4.4.9

7.7.2 รายงานประจำเดือน สรุปผลการดำเนินการจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ 4.4.10

7.7.3 รายงานประจำเดือน สรุปผลการตอบสนองต่อภัยคุกคามสำหรับเครื่องแม่ข่ายและเครื่องลูกข่าย (MDR) ตามข้อ 4.7

8. เกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ในการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์โครงการจ้างบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ และทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศ กนอ. ประจำปี 2565 ครั้งนี้ ลักษณะงานเป็นการตรวจสอบช่องโหว่ (VA) และทดสอบเจาะระบบ (Penetration Testing) ระบบสารสนเทศของ กนอ. รวมถึงให้บริการบริการศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operation Center : SOC) และตอบสนองต่อภัยคุกคาม

สำหรับเครื่องแม่ข่ายและเครื่องลูกข่ายของ กนอ. ซึ่งข้อเสนอเกี่ยวกับแนวคิด วิธีการดำเนินงานตามขอบเขตของงาน รวมถึงกระบวนการขั้นตอนที่ใช้ในการเฝ้าระวังภัยคุกคามทางไซเบอร์ให้กับทาง กนอ. ไม่อยู่บนพื้นฐานเดียวกัน ส่งผลให้เกิดปัญหาในการพิจารณาคัดเลือกข้อเสนอ จึงกำหนดให้มีการยื่นข้อเสนอด้านเทคนิคเพื่อพิจารณาคัดเลือกข้อเสนอด้านเทคนิคต้องผ่านเกณฑ์ขั้นต่ำก่อน ตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 มาตรา 65 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ 2560 ข้อ 83 (3) และผู้ยื่นข้อเสนอที่ผ่านการพิจารณาข้อเสนอด้านเทคนิคแล้ว กนอ. จะพิจารณาด้วยเกณฑ์ราคาและเกณฑ์อื่นๆ (ข้อเสนอด้านเทคนิค) ซึ่งมีสัดส่วนน้ำหนักระหว่างเกณฑ์ด้านราคาเท่ากับร้อยละ 20 และเกณฑ์อื่นๆ (ข้อเสนอด้านเทคนิค) ร้อยละ 80 โดยคณะกรรมการประกวดราคาอิเล็กทรอนิกส์จะดำเนินการเมื่อสิ้นสุดระยะเวลาการเสนอราคาในระบบอิเล็กทรอนิกส์แล้วตามลำดับ ดังนี้

8.1 จัดพิมพ์เอกสารข้อเสนอทั้งหมดของผู้ยื่นข้อเสนอทุกรายการจากระบบการประกวดราคา อิเล็กทรอนิกส์ (ยกเว้นเอกสารข้อเสนอด้านราคา) จำนวน 1 ชุด และลงลายมือชื่อกำกับไว้ทุกแผ่น

8.2 ตรวจสอบการมีผลประโยชน์ร่วมกัน และความครบถ้วนถูกต้องของเอกสารหลักฐานต่างๆ แล้ว พิจารณาคัดเลือกรายที่ไม่มีผลประโยชน์ร่วมกัน มีคุณสมบัติและเอกสารหลักฐานต่างๆ ครบถ้วนถูกต้องและพิจารณาข้อเสนอด้านเทคนิคตามเกณฑ์การให้คะแนนที่กำหนดต่อไป สำหรับรายที่มีผลประโยชน์ร่วมกัน หรือมีคุณสมบัติหรือยื่นเอกสารหลักฐานต่างๆ ไม่ครบถ้วนถูกต้อง หรือไม่ครบถ้วน หรือยื่นข้อเสนอไม่ถูกต้อง คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ จะไม่พิจารณาข้อเสนอด้านเทคนิคของผู้ยื่นข้อเสนอรายนั้น เว้นแต่เป็น ข้อผิดพลาด หรือผิดหลงเพียงเล็กน้อย หรือผิดแผกไปจากเงื่อนไขของเอกสารประกวดราคาอิเล็กทรอนิกส์ในส่วนที่ มิใช่สาระสำคัญเฉพาะในกรณีที่พิจารณาเห็นว่าจะเป็นประโยชน์ต่อ กนอ. เท่านั้น

8.3 พิจารณาข้อเสนอด้านเทคนิคของผู้ยื่นข้อเสนอทุกรายที่ผ่านการพิจารณาตามข้อ 8.2 และทำการประเมินข้อเสนอด้านเทคนิคโดยมีสัดส่วนน้ำหนักในการให้คะแนนรวมร้อยละ 100 โดยมีคะแนนและสัดส่วนน้ำหนักในการให้คะแนนแต่ละหัวข้อ ดังนี้

(1) ความรู้ความเข้าใจด้าน SOC เพื่อตอบโจทย์การเฝ้าระวังในปัจจุบันและอนาคตของ กนอ.
100 คะแนน น้ำหนักร้อยละ 40

(2) ความรู้ความเข้าใจด้าน SOC เพื่อตอบโจทย์วิสัยทัศน์ ของ กนอ.
100 คะแนน น้ำหนักร้อยละ 40

(3) คุณวุฒิและประสบการณ์ของบุคลากร
100 คะแนน น้ำหนักร้อยละ 15

(4) ผลงานของผู้ยื่นข้อเสนอ
100 คะแนน น้ำหนักร้อยละ 5

ทั้งนี้ ในการพิจารณาให้คะแนนตามหัวข้อต่างๆ ข้างต้น คณะกรรมการฯ จะพิจารณาความครบถ้วนในเนื้อหาวิธีการดำเนินงานตามขอบเขตของงาน และพิจารณาเปรียบเทียบระหว่างข้อเสนอของผู้ยื่นข้อเสนอด้วยกัน รวมทั้งคณะกรรมการฯ จะเชิญผู้ยื่นข้อเสนอให้มาอธิบายรายละเอียดข้อเสนอทางเทคนิค รวมทั้งชี้แจง และตอบข้อซักถามเพิ่มเติม (ถ้ามี) เพื่อประกอบการพิจารณาด้วย ข้อเสนอที่ดีที่สุดจะได้คะแนนในหัวข้อนั้นๆ มากที่สุด ข้อเสนอของผู้ยื่นข้อเสนอรายอื่นจะได้คะแนนลดหลั่นลงไปตามความเหมาะสม หรือสัดส่วน **รายละเอียดหัวข้อและหัวข้อย่อยในการให้คะแนนข้อเสนอด้านเทคนิค ตามภาคผนวก ข** ทั้งนี้ ข้อเสนอด้านเทคนิคที่ผ่านเกณฑ์การพิจารณาจะต้องได้รับคะแนนสัดส่วนน้ำหนักรวมไม่น้อยกว่าร้อยละ 80

8.4 ข้อเสนอด้านเทคนิคที่ผ่านเกณฑ์การพิจารณาตามข้อ 8.3 จะได้รับการประเมินค่าประสิทธิภาพต่อราคา (Price Performance) อีกครั้งหนึ่งตามสัดส่วนเกณฑ์ราคาและเกณฑ์ข้อเสนอด้านเทคนิคที่กำหนด โดยข้อเสนอด้านราคาจะให้คะแนนตามช่วงความต่างของราคาที่เสนอแต่ละราย ทั้งนี้ ระบบการจัดซื้อจัดจ้างภาครัฐ (Electronic Government Procurement : e-GP) จะพิจารณาให้คะแนนเกณฑ์ราคาและเกณฑ์อื่น (ข้อเสนอด้านเทคนิค) ในระบบ หลังจากนั้นระบบจะจัดเรียงตามคะแนนไว้ 3 ลำดับ ผู้ยื่นข้อเสนอที่ได้รับคะแนนประเมินรวมสูงสุดจะได้รับการคัดเลือก และ กนอ. จะพิจารณาเจรจาต่อรองราคาตามที่เห็นสมควรเพื่อประโยชน์ของ กนอ. ต่อไป

8.5 กรณีผู้ได้รับการคัดเลือกไม่ไปทำสัญญาภายในวันเวลาที่กำหนด กนอ. จะพิจารณา เรียกรายลำดับถัดไปเพื่อเจรจาต่อรองและ/หรือทำสัญญาต่อไป หรืออาจพิจารณายกเลิกการประกาศเชิญชวน เพื่อดำเนินการใหม่ตามวิธีหรือขั้นตอนตามระเบียบที่เกี่ยวข้องต่อไป

9. เงื่อนไขการชำระเงิน

9.1 งวดที่ 1 กนอ. จะจ่ายเงินจำนวนร้อยละ 15 ของวงเงินค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงานตามข้อ 7.1 และ 7.2 แล้วเสร็จ และคณะกรรมการตรวจรับพัสดุ ได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

9.2 งวดที่ 2 กนอ. จะจ่ายเงินจำนวนร้อยละ 15 ของวงเงินค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงาน ตามข้อ 7.3 แล้วเสร็จ และคณะกรรมการตรวจรับพัสดุ ได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

9.3 งวดที่ 3 กนอ. จะจ่ายเงินจำนวนร้อยละ 15 ของวงเงินค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงาน ตามข้อ 7.4 แล้วเสร็จ และคณะกรรมการตรวจรับพัสดุ ได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

9.4 งวดที่ 4 กนอ. จะจ่ายเงินจำนวนร้อยละ 15 ของวงเงินค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงาน ตามข้อ 7.5 แล้วเสร็จ และคณะกรรมการตรวจรับพัสดุ ได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

9.5 งวดที่ 5 กนอ. จะจ่ายเงินจำนวนร้อยละ 20 ของวงเงินค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงาน ตามข้อ 7.6 แล้วเสร็จ และคณะกรรมการตรวจรับพัสดุ ได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

9.6 งวดที่ 6 กนอ. จะจ่ายเงินจำนวนร้อยละ 20 ของวงเงินค่าจ้างตามสัญญา เมื่อผู้รับจ้างได้ปฏิบัติงาน ตามข้อ 7.7 แล้วเสร็จ และคณะกรรมการตรวจรับพัสดุ ได้ตรวจสอบรับรองครบถ้วนถูกต้องเรียบร้อยแล้ว

10. การปรับเนื่องจากงานล่าช้าและการรับประกันคุณภาพการให้บริการ (Service Level Agreement)

10.1 ในกรณีผู้รับจ้างไม่สามารถส่งมอบงานทั้งหมดหรือบางส่วนได้ในข้อ 7 โดยไม่ได้เกิดจากความล่าช้าหรือความไม่พร้อมในการตรวจรับของ กนอ. ผู้รับจ้างต้องชำระค่าปรับเป็นรายวันในอัตราร้อยละ 0.1 ของมูลค่างานตามสัญญา จนกว่าจะดำเนินการแล้วเสร็จและได้รับความความเห็นชอบจาก กนอ.

10.2 ในกรณีผู้รับจ้างไม่สามารถซ่อมแซมแก้ไขให้ระบบ EDR ตามข้อ 4.6 สามารถกลับมาใช้งานได้ดีดังเดิมภายในเวลาไม่เกิน 7 วันทำการ นับถัดจากวันที่ได้รับแจ้งความชำรุดบกพร่อง กนอ. จะปรับเป็นรายชั่วโมงในอัตราร้อยละ 0.025 ของราคาค่าจ้างทั้งหมดตามสัญญา เศษของชั่วโมงให้นับเป็น 1 ชั่วโมง

11. ระยะเวลาการดำเนินงาน

ผู้รับจ้างต้องปฏิบัติงานภายใต้ข้อกำหนดและขอบเขตงานฉบับนี้เป็นระยะเวลา 420 วัน นับถัดจากวันลงนามในสัญญา

12. เงื่อนไขอื่น ๆ

ผู้ยื่นข้อเสนอต้องยื่นเอกสารประกอบการพิจารณาที่เกี่ยวข้อง โดยต้องส่งเอกสารมาพร้อมกับการยื่นเอกสารคุณลักษณะของการประกวดราคาอิเล็กทรอนิกส์ในครั้งนี้ ประกอบด้วย

12.1 สำเนาเอกสารแคตตาล็อกของระบบ EDR หรือรายการอื่นๆ ที่เกี่ยวข้องในโครงการ เป็นเอกสารภาษาไทยและ/หรือภาษาอังกฤษ ที่จัดทำขึ้นโดยผู้ผลิตที่เสนอมาเท่านั้น ทั้งนี้สามารถพิมพ์แคตตาล็อกที่ถูกจัดทำไว้ในเว็บไซต์ของผู้ผลิตได้ เอกสารแคตตาล็อกทั้งหมดต้องจัดเรียงและกำหนดเลขหน้าให้ชัดเจน โดยให้ขีดเส้นใต้และเขียนเลขหัวข้อตามคุณลักษณะ หากมีรายการคุณลักษณะใดที่ไม่ปรากฏในแคตตาล็อก ต้องมีหนังสือรับรองจากผู้ผลิตรับรองคุณลักษณะดังกล่าวไว้อย่างชัดเจน โดยแนบต่อท้ายแคตตาล็อกของแต่ละรายการ

12.2 ผู้ยื่นข้อเสนอต้องเป็นตัวแทนจำหน่ายระบบ EDR ที่ได้รับการแต่งตั้งจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยที่ถูกต้องตามกฎหมาย

12.3 จัดทำเอกสารตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะที่เสนอมา ทุกรายการ กับรายละเอียดคุณลักษณะของครุภัณฑ์ของผู้ยื่นข้อเสนอ การเสนอในรายละเอียดที่ผู้ยื่นข้อเสนอ เสนอนั้นจะต้องระบุยี่ห้อและรุ่นของครุภัณฑ์ที่เสนอมาของแต่ละรายการครุภัณฑ์ไว้อย่างชัดเจน และในแต่ละรายการคุณลักษณะ ให้ระบุเลขหน้าของเอกสารแคตตาล็อก ไว้ในช่องเอกสารอ้างอิง (ระบุเลขหน้า)

12.4 การเสนอคุณลักษณะที่เทียบเท่าหรือดีกว่าในรายการครุภัณฑ์ที่เสนอมาข้างต้น ในกรณีที่เสนอคุณลักษณะไม่ตรงตามที่ กนอ. กำหนด แต่เป็นการเสนอคุณลักษณะที่เทียบเท่าหรือดีกว่า ผู้ยื่นข้อเสนอต้องจัดทำเอกสารเปรียบเทียบคุณลักษณะดังกล่าวพร้อมแนบเอกสารมาพร้อมหนังสือรับรองด้วย

12.5 หนังสือรับรองมาตรฐาน ISO/IEC 27001:2013 สำหรับศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Security Operations Center: SOC ซึ่งตั้งอยู่ในประเทศไทยของผู้รับจ้าง ตามที่ระบุไว้ในข้อกำหนดและขอบเขตของงานข้อ 3.11

12.6 หนังสือรับรองผลงานหรือสำเนาสัญญาฯ ตามที่ระบุไว้ในข้อกำหนดและขอบเขตของงานข้อ 3.12

12.7 จำนวนและคุณสมบัติของบุคลากร โดยระบุชื่อ ตำแหน่ง หน้าที่รับผิดชอบให้ชัดเจน พร้อมแนบเอกสารประวัติบุคคลแสดงวุฒิการศึกษา ประสบการณ์การทำงาน ใบรับรองความรู้ความสามารถ โดยมีรายละเอียดอย่างน้อยตามภาคผนวก ก

13. วงเงินงบประมาณ

งบประมาณทั้งสิ้น 7,000,000 บาท (เจ็ดล้านบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่มแล้ว โดยเป็นงบประมาณประจำปี 2565

ภาคผนวก ก

คุณสมบัติบุคลากร

ตำแหน่ง	คุณสมบัติ	จำนวน (คน)
1 หัวหน้าโครงการ	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ ITIL V4 - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 5 ปี	1
2. ที่ปรึกษาด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ Certified Information System Security Professional (CISSP) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 7 ปี	1
3. หัวหน้าประจำศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Head of SOC)	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ Certified Ethical Hacker (CEH) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 5 ปี	1
4 ผู้เชี่ยวชาญด้านการทดสอบเจาะระบบ	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ Offensive Security Certified Professional (OSCP) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 3 ปี	1
5. ผู้ปฏิบัติงานด้านการทดสอบเจาะระบบ	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ Certified Ethical Hacker (CEH) - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 3 ปี	1
6. เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 3	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ต้องได้รับใบรับรองความรู้ความสามารถ CompTIA CASP+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 4 ปี	2

ตำแหน่ง	คุณสมบัติ	จำนวน (คน)
7. เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 2	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ CompTIA CySA+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 2 ปี	3
8. เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 1	- วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี ด้านเทคโนโลยีสารสนเทศ หรือสาขาที่เกี่ยวข้อง - ได้รับใบรับรองความรู้ความสามารถ CompTIA Security+ - มีประสบการณ์ทำงานด้านเทคโนโลยีสารสนเทศ 1 ปี	8

ภาคผนวก ข

หลักเกณฑ์การประเมินค่าประสิทธิภาพต่อราคา (Price Performance)

รายละเอียดการนำเสนอทางเทคนิค

ลำดับ	หลักเกณฑ์พิจารณา	คะแนน
1	อธิบาย Security Operations Center ที่จะมีการให้บริการจากท่าน เพื่อตอบโจทย์ การเฝ้าระวังในปัจจุบันและอนาคตของ กนอ. ได้อย่างไร และมีกระบวนการขั้นตอนที่ใช้ในการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างไรให้กับทาง กนอ. (คะแนนเต็ม 100 คะแนน น้ำหนัก 40)	
	- เนื้อหาไม่ครบถ้วนหรือมีประเด็นใดประเด็นหนึ่งผิดไปจากหลักวิชาการ	0
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจทั้ง 3 คำถาม	60
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจทั้ง 3 คำถาม - มีการแสดงตัวอย่างการดำเนินการตามเงื่อนไข (Use Case) ที่ใช้ในเฝ้าระวังภัยคุกคามทั้ง 3 คำถาม	70
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจทั้ง 3 คำถาม - มีการแสดงตัวอย่างการดำเนินการตามเงื่อนไข (Use Case) ที่ใช้ในเฝ้าระวังภัยคุกคามทั้ง 3 คำถาม - มีการอธิบายประโยชน์ที่ กนอ. จะได้รับได้อย่างครบถ้วน	80
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจทั้ง 3 คำถาม - มีการแสดงตัวอย่างการดำเนินการตามเงื่อนไข (Use Case) ที่ใช้ในเฝ้าระวังภัยคุกคามทั้ง 3 คำถาม - มีการอธิบายประโยชน์ที่ กนอ. จะได้รับได้อย่างครบถ้วน - มีการแสดงตัวอย่างการดำเนินการในประเทศไทยที่ประสบความสำเร็จ	100
2	อธิบาย Security Operations Center ที่จะมีการให้บริการจากท่าน เพื่อตอบโจทย์วิสัยทัศน์ ของ กนอ. ในเรื่องดังต่อไปนี้ (1) e-PP/ERP (2) Digital Twin (3) Governance Server Platform (4) Data Governance (5) Open Government Data (6) Industrial Estate Open Data (คะแนนเต็ม 100 คะแนน น้ำหนัก 40)	
	- เนื้อหาไม่ครบถ้วนหรือมีประเด็นใดประเด็นหนึ่งผิดไปจากหลักวิชาการ	0
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจของการบริการของท่าน ให้สอดคล้องทั้ง 6 หัวข้อ	60
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจเบื้องต้น ทั้ง 6 หัวข้อ	70
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจเป็นอย่างดี ทั้ง 6 หัวข้อ - มีการอธิบายประโยชน์ที่ กนอ. จะได้รับได้อย่างครบถ้วน	80
	- มีการอธิบายเพื่อแสดงถึงความรู้ความเข้าใจเป็นอย่างดี ทั้ง 6 หัวข้อ - มีการอธิบายประโยชน์ที่ กนอ. จะได้รับได้อย่างครบถ้วน - มีการอธิบายเพื่อทำให้ทาง กนอ. มั่นใจ ที่ผู้รับจ้างจะสามารถตอบโจทย์วิสัยทัศน์ของทาง กนอ. ได้ทั้งในปัจจุบันและอนาคต	100

ลำดับ	หลักเกณฑ์พิจารณา	คะแนน
3	คุณวุฒิและประสบการณ์ของบุคลากรโดยพิจารณาจากคุณวุฒิและประสบการณ์ของบุคลากรที่ตรงหรือใกล้เคียงตามข้อเสนอด้านเทคนิคที่สุด (คะแนน 100 น้ำหนัก 15)	
	3.1 หัวหน้าโครงการ	(คะแนน 15)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	12
	- มีคุณวุฒิและประสบการณ์ของบุคลากรที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	13-15
	3.2 ที่ปรึกษาด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์	(คะแนน 15)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	12
	- มีคุณวุฒิและประสบการณ์ของบุคลากรที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	13-15
	3.3 หัวหน้าประจำศูนย์เฝ้าระวังความปลอดภัยทางไซเบอร์ (Head of SOC)	(คะแนน 15)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	12
	- มีคุณวุฒิและประสบการณ์ของบุคลากนที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	13-15
	3.4 ผู้เชี่ยวชาญด้านการทดสอบเจาะระบบ	(คะแนน 15)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	12
	- มีคุณวุฒิและประสบการณ์ของบุคลากรที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	13-15
	3.5 ผู้ปฏิบัติงานด้านการทดสอบเจาะระบบ	(คะแนน 10)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	8
	- มีคุณวุฒิและประสบการณ์ของบุคลากรที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	9-10
	3.6 เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 3	(คะแนน 10)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	8
	- มีคุณวุฒิและประสบการณ์ของบุคลากนที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	9-10
	3.7 เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 2	(คะแนน 10)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	8
	- มีคุณวุฒิและประสบการณ์ของบุคลากรที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	9-10
	3.8 เจ้าหน้าที่ปฏิบัติการและวิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Analyst) ระดับ 1	(คะแนน 10)
	- มีคุณวุฒิและประสบการณ์ของบุคลากรตามข้อกำหนด	8
	- มีคุณวุฒิและประสบการณ์ของบุคลากรที่ดีกว่าข้อกำหนด โดยเปรียบเทียบกับผู้ยื่นข้อเสนอด้วยกัน	9-10

ลำดับ	หลักเกณฑ์พิจารณา	คะแนน
4	ผลงานของผู้ยื่นข้อเสนอ (คะแนนเต็ม 100 คะแนน น้ำหนัก 5)	
	- มีผลงานในการให้บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือให้บริการสอดคล้องกับขอบเขตงาน ซึ่งเป็นผลงานที่แล้วเสร็จไม่เกิน 5 ปี นับถึงวันยื่นข้อเสนอ และเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ รัฐวิสาหกิจหรือหน่วยงานเอกชนที่ กนอ. เชื่อถือ จำนวน 1 โครงการ ซึ่งมูลค่าของโครงการไม่น้อยกว่า 3,000,000 บาท (สามล้านบาทถ้วน)	80
	- มีผลงานในการให้บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือให้บริการสอดคล้องกับขอบเขตงาน ซึ่งเป็นผลงานที่แล้วเสร็จไม่เกิน 5 ปี นับถึงวันยื่นข้อเสนอ และเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ รัฐวิสาหกิจหรือหน่วยงานเอกชนที่ กนอ. เชื่อถือ จำนวน 2-3 โครงการ ซึ่งมูลค่าของโครงการไม่น้อยกว่า 3,000,000 บาท (สามล้านบาทถ้วน)	90
	- มีผลงานในการให้บริการเฝ้าระวังด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือให้บริการสอดคล้องกับขอบเขตงาน ซึ่งเป็นผลงานที่แล้วเสร็จไม่เกิน 5 ปี นับถึงวันยื่นข้อเสนอ และเป็นคู่สัญญาโดยตรงกับหน่วยงานของรัฐ รัฐวิสาหกิจหรือหน่วยงานเอกชนที่ กนอ. เชื่อถือ จำนวนมากกว่า 3 โครงการ ซึ่งมูลค่าของโครงการไม่น้อยกว่า 3,000,000 บาท (สามล้านบาทถ้วน)	100