กองทุนบำเหน็จบำนาญข้าราชการ

ขอบเขตของงาน (Term of Reference)

การจ้างผู้ให้บริการเฝ้าระวังและแก้ไขเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ

---

1. หลักการและเหตุผล

จากความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศ ซึ่งถูกนำมาใช้ประโยชน์ในการดำเนินธุรกิจและการติดต่อสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์ ระบบคลาวด์ และอินเตอร์เน็ต จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็ว และปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายให้ทั้งในระดับบุคคล ระดับองค์กร และระดับประเทศ ดังนั้น กองทุนบำเหน็จบำนาญข้าราชการ (กบข.) จำเป็นต้องเตรียมการป้องกันและรับมือภัยคุกคามและความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่อาจจะเกิดขึ้นได้อย่างทันท่วงที แก้ไขเหตุการณ์ภัยคุกคามได้อย่างรวดเร็วและเหมาะสม ทันต่อสถานการณ์ ตลอดจนมีการดูแลรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์อย่างต่อเนื่อง

กบข. จึงเห็นควรจัดจ้างผู้ให้บริการเฝ้าระวังและแก้ไขเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ โดยมีระยะเวลาสัญญา 2 ปี 3 เดือน ตั้งแต่วันที่ 1 พฤษภาคม 2565 จนถึงวันที่ 31 กรกฎาคม 2567

2. วัตถุประสงค์

การจ้างผู้ให้บริการเฝ้าระวังและแก้ไขเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ เพื่อปฏิบัติงานดังนี้

2.1 วิเคราะห์ เฝ้าระวัง แจ้งเตือน รับมือ และร่วมแก้ไขปัญหาที่เกิดจากภัยคุกคามหรือเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่อาจจะก่อให้เกิดความเสียหายต่อข้อมูล ระบบสารสนเทศและโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของ กบข. ได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยที่ได้ตามมาตรฐานสากล สามารถรับมือและแก้ไขเหตุการณ์ภัยคุกคามได้อย่างรวดเร็วและเหมาะสม ทันต่อสถานการณ์

2.2 ให้การสนับสนุนด้านเทคนิคแก่ กบข. เยี่ยงมืออาชีพในการเฝ้าระวัง แจ้งเตือน รับมือ และร่วมแก้ไขเหตุการณ์ภัยคุกคามและความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ ตลอดจนมีการดูแลรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์อย่างเหมาะสมและต่อเนื่อง

2.3 เพื่อยกระดับมาตรฐานให้มีการตอบสนองต่อภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ในรูปแบบอัตโนมัติ โดย กบข. มีระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ที่มีประสิทธิภาพในการวิเคราะห์และแก้ไขเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ได้อย่างรวดเร็วและเหมาะสม ทันต่อสถานการณ์

3. คุณสมบัติผู้ยื่นข้อเสนอ

ผู้ยื่นข้อเสนอต้องมีคุณสมบัติตามมาตรฐานที่ระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) กำหนด

4. รายการรายละเอียดของงานจ้าง

ผู้ให้บริการต้องดำเนินการเฝ้าระวังและแก้ไขเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ โดยมีระยะเวลาสัญญา 2 ปี 3 เดือน ตั้งแต่วันที่ 1 พฤษภาคม 2565 จนถึงวันที่ 31 กรกฎาคม 2567 โดยมีรายละเอียดการดำเนินการ ดังนี้

4.1 การดำเนินการระยะที่ 1 การเตรียมการก่อนการให้บริการ (Implementation) เฝ้าระวังตอบสนองและแก้ไขต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) โดยมีระยะเวลาดำเนินการ 3 เดือน ตั้งแต่วันที่ 1 พฤษภาคม 2565 จนถึงวันที่ 31 กรกฎาคม 2565 ซึ่งมีรายละเอียดดังนี้

4.1.1 ผู้ให้บริการต้องนำผลการทำ Risk Assessment ที่ กบข. มีอยู่ หรือจัดทำ Risk Assessment เพื่อมาทำการประเมินในการจัดทำ Playbook

4.1.2 ผู้ให้บริการต้องจัดเตรียมข้อมูลต่าง ๆ ที่จะร้องขอกับทาง กบข. เพื่อให้ทาง กบข. จัดเตรียมความพร้อม เช่น VPN, Firewall Port และ IP Address เป็นต้น

4.1.3 ผู้ให้บริการต้องจัดส่งข้อมูลในกรณีที่มีการนำอุปกรณ์มาติดตั้งที่ กบข. เช่น จำนวนของอุปกรณ์, Specification ของอุปกรณ์ และ Serial Number ของอุปกรณ์ เป็นต้น

4.1.4 ผู้ให้บริการต้องดำเนินการติดตั้งระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) พร้อมทำการเชื่อมต่อกับอุปกรณ์ที่ กบข. มีการใช้งานอยู่อย่างเหมาะสม

4.1.5 ผู้ให้บริการต้องดำเนินการติดตั้งระบบวิเคราะห์และตอบสนองต่อภัยคุกคามของระบบเครือข่ายและเครื่องคอมพิวเตอร์ (Extended Detection and Response: XDR) โดยเครื่องที่ทาง กบข. ต้องการให้ติดตั้งจะต้องมีคุณสมบัติตรงตามความต้องการของระบบ

4.1.6 สรุปรายงานการเตรียมการก่อนการให้บริการ (Implementation)

4.2 การดำเนินการระยะที่ 2 การให้บริการ ผู้ให้บริการต้องเฝ้าระวังตอบสนองและแก้ไขต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) เป็นระยะเวลา 2 ปี ตั้งแต่วันที่ 1 สิงหาคม 2565 จนถึงวันที่ 31 กรกฎาคม 2567 โดยมีรายละเอียดดังนี้

4.2.1 ผู้ให้บริการต้องให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามทางไซเบอร์ จากระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information and Event Management: SIEM) ที่ กบข. มีการใช้งานอยู่ โดยให้บริการแจ้งเตือนผ่านระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) และแก้ไขเหตุการณ์ร่วมกับ กบข. เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ ตลอดระยะเวลาสัญญาตามเงื่อนไขต่อไปนี้

ระดับความรุนแรง	การแจ้งเตือนผ่านระบบ	การร่วมแก้ไขปัญหา
Critical	ระบบทำการแจ้งเตือนให้ทาง กบข. รับทราบ ภายใน 5 นาที	ดำเนินการแก้ไขปัญหาเฉพาะหน้าร่วมกับ กบข. ภายใน 4 ชั่วโมง และดำเนินการต่อเนื่องจนแล้วเสร็จ พร้อมเสนอแนวทางการป้องกันตามที่ กบข. ร้องขอ
High	ระบบทำการแจ้งเตือนให้ทาง กบข. รับทราบ ภายใน 10 นาที	ดำเนินการแก้ไขปัญหาเฉพาะหน้าร่วมกับ กบข. ภายใน 8 ชั่วโมง และดำเนินการต่อเนื่องจนแล้วเสร็จ พร้อมเสนอแนวทางการป้องกันตามที่ กบข. ร้องขอ
Medium	ระบบทำการแจ้งเตือนให้ทาง กบข. รับทราบ ภายใน 1 ชั่วโมง	ให้คำปรึกษารวมถึงแนะนำการแก้ไขกับ กบข. ภายใน 7 วัน
Low	ระบบทำการแจ้งเตือนให้ทาง กบข. รับทราบ ภายใน 24 ชั่วโมง	ให้คำปรึกษารวมถึงแนะนำการแก้ไขกับ กบข. ภายใน 30 วัน

เกณฑ์ในการกำหนดระดับความรุนแรงต้องมีการกำหนดขอบเขตร่วมกับ กบข. ซึ่งแบ่งออกเป็น 4 ระดับดังต่อไปนี้

Critical - ผลกระทบกับกลุ่มระบบสารสนเทศที่ทำให้การดำเนินธุรกิจหยุดชะงัก และจำเป็นจะต้องแก้ไขอย่างเร่งด่วนที่สุด

High - ผลกระทบกับกลุ่มระบบสารสนเทศที่มีผลกระทบต่อการดำเนินธุรกิจ และมีความจำเป็นต้องแก้ไขอย่างเร่งด่วน

Medium - ผลกระทบกับประสิทธิภาพการทำงานของกลุ่มระบบสารสนเทศ โดยไม่มีผลกระทบต่อการดำเนินธุรกิจ

Low - ผลกระทบกับกลุ่มระบบสารสนเทศทางเทคนิค โดยไม่มีผลกระทบต่อการดำเนินธุรกิจ หรือการปฏิบัติงานภายในสำนักงาน

4.2.2 ผู้ให้บริการต้องให้บริการเฝ้าระวังตอบสนองและแก้ไขต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) ผ่านช่องทางการเฝ้าระวังระยะไกล (Remote) หรือเข้ามาปฏิบัติงานในสำนักงาน กบข. เพื่อแก้ไขปัญหาในกรณีที่มีระดับความรุนแรงเป็น Critical หรือ High ตามที่ กบข.ร้องขอ

4.2.3 ผู้ให้บริการต้องจัดให้มีเจ้าหน้าที่เพื่อดำเนินการเฝ้าระวังภัยคุกคามและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) ตั้งแต่วันที่ 1 สิงหาคม 2565 จนถึงวันที่ 31 มกราคม 2566

4.2.4 ผู้ให้บริการต้องดำเนินการเฝ้าระวังและตอบสนองต่อภัยคุกคามทางไซเบอร์ (Cyber Security Monitoring Services) โดยระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) และผู้เชี่ยวชาญ (Security Analyst) ตั้งแต่วันที่ 1 กุมภาพันธ์ 2566 จนถึงวันที่ 31 กรกฎาคม 2567

4.2.5 ผู้ให้บริการต้องจัดให้มีเจ้าหน้าที่ผู้เชี่ยวชาญที่มีความรู้ความสามารถด้านภัยคุกคามทางไซเบอร์ เพื่อให้คำแนะนำในการปรับแก้ไข Playbook ให้แก่เจ้าหน้าที่ของ กบข. ตลอดระยะเวลาสัญญา

4.2.6 ผู้ให้บริการต้องจัดทำ Playbook บนระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) จำนวนไม่น้อยกว่า 15 Playbooks เพื่อให้มีกระบวนการในการตอบสนองที่เท่าทันกับภัยคุกคามที่เกิดขึ้นในรูปแบบใหม่ ๆ ตลอดระยะเวลาสัญญา โดยมีรายละเอียด ดังนี้

4.2.6.1 จัดทำ 5 Playbooks ภายในวันที่ 31 มกราคม 2566

4.2.6.2 จัดทำ 10 Playbooks ภายในวันที่ 31 มกราคม 2567

4.2.7 ผู้ให้บริการต้องจัดทำรายงานประจำวัน (Daily Report), รายงานประจำเดือน (Monthly Report), รายงานสรุปรายไตรมาสหรือทุกรอบระยะเวลา 3 เดือน (Quarterly Report) และรายงานสรุปประจำปี (Yearly Report) และนำส่งรายงานให้แก่ กบข. ภายในระยะเวลาที่กำหนด โดยมีรายงานอย่างน้อยดังต่อไปนี้

4.2.7.1 รายงานการแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) ให้ กบข. ทราบ

4.2.7.2 รายงานประจำวัน (Daily Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด โดยรายงานเหตุการณ์ผิดปกติหรือภัยคุกคามคุกคาม

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) โดยมีการจัดระดับความรุนแรง และสรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT Security & Cybersecurity Incident Management) ที่เกิดขึ้นในแต่ละวัน ภายในเวลา 06:30 น. ของทุกวัน

4.2.7.3 รายงานประจำเดือน (Monthly Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด ภายในวันที่ 5 ของเดือนถัดไป โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT Security & Cybersecurity Monitoring) ในแต่ละเดือน

(ข) สรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกิดขึ้นในแต่ละเดือน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กบข.

(ค) สรุปการแจ้งเตือนเหตุการณ์ผิดปกติหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) และสรุปสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Incident Management) ที่เกิดขึ้นในแต่ละเดือน

(ง) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) ที่เกิดขึ้นในแต่ละเดือน (ถ้ามี)

4.2.7.4 รายงานสรุปรายไตรมาส หรือทุกรอบระยะ 3 เดือน (Quarterly Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด ภายใน 15 วัน นับจากวันที่สิ้นสุดไตรมาส หรือรอบระยะเวลาทุก 3 เดือน โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT Security & Cybersecurity Monitoring) ในแต่ละไตรมาส หรือทุกรอบระยะเวลา 3 เดือน

(ข) สรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกิดขึ้นในแต่ละไตรมาส หรือทุกรอบระยะเวลา 3 เดือน โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กบข.

(ค) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) ที่เกิดขึ้นในแต่ละไตรมาส หรือทุกรอบระยะวเลา 3 เดือน (ถ้ามี)

4.2.7.5 รายงานสรุปประจำปี (Yearly Report)

ผู้ให้บริการต้องจัดทำรายงานเป็นไฟล์ข้อมูลอิเล็กทรอนิกส์ และจัดส่งรายงานให้แก่ กบข. ผ่านช่องทาง e-mail หรือช่องทางอื่นใดที่ กบข. กำหนด ภายใน 20 วัน นับจากวันสิ้นปี โดยมีรายละเอียดของรายงานเป็นอย่างน้อย ครอบคลุมถึง

(ก) บทสรุปผู้บริหาร (Executive Summary) เพื่อรายงานผลการเฝ้าระวังภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT Security & Cybersecurity Monitoring) โดยสรุปเป็นภาพรวมทั้งปี

(ข) สรุปเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่เกิดขึ้นทั้งหมดภายในปี โดยมีการจัดระดับความรุนแรง และวิเคราะห์ผลกระทบต่อการดำเนินธุรกิจของ กบข.

(ค) สรุปการดำเนินการแจ้งเตือนเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) และรายงานสถานะการดำเนินการบริหารจัดการภัยคุกคามที่พบหรือความผิดปกติที่กระทบต่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (IT Security Incident Management) ที่เกิดขึ้นเป็นภาพรวมทั้งปี

(ง) อัพเดทข้อมูลข่าวสารเกี่ยวกับภัยคุกคามร้ายแรงด้านความปลอดภัยสารสนเทศ (Security News) และสรุปแนวโน้ม หรือ Trend ของภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารและข้อแนะนำที่ กบข. ควรดำเนินการเพื่อรับมือกับภัยคุกคามเหล่านั้น

4.2.8 ผู้ให้บริการมีระบบเฝ้าระวัง วิเคราะห์และตอบสนองต่อภัยคุกคาม (Extended Detection and Response: XDR) เพื่อการเฝ้าระวังภัยคุกคามในภาพรวมทั้งในส่วนของระบบเครือข่าย (Network) และเครื่องคอมพิวเตอร์ (Endpoint) จำนวนไม่น้อยกว่า 400 สิทธิ์ โดยจัดอยู่ในกลุ่ม Leader หรือ Strong Performer ของ Gartner หรือ Forrester : Extended Detection and Response (XDR) ปี 2021 หรือปีล่าสุด และสามารถทำงานร่วมกับระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) อย่างมีประสิทธิภาพ

4.2.9 ผู้ให้บริการต้องมีเครื่องมือที่สามารถนำส่งรายการช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) และ Asset Inventory ต่าง ๆ ของเครื่อง เช่น OS, Application, User, Disk, RAM เป็นอย่างน้อย โดยครอบคลุมระบบปฏิบัติการ Windows, Windows Server, และ Linux จำนวนไม่น้อยกว่า 400 สิทธิ์

4.2.10 ผู้ให้บริการต้องมีเครื่องมือที่มีความสามารถวิเคราะห์ภัยคุกคาม ได้อย่างน้อยดังนี้

4.2.10.1 Behavioral analytics เพื่อตรวจจับ anomalies indicative of attack ด้วยการวิเคราะห์ข้อมูลจาก Endpoint events และ User event over time

4.2.10.2 User and Entity Behavior Analytics (UEBA) หรือ User behavior analytics (UBA)

4.2.10.3 มี Machine Learning และ Cloud Sandboxing ในการวิเคราะห์ Unknown Threat แบบ Real-Time

4.2.10.4 สามารถแสดงแผนภูมิของภัยคุกคามที่ตรวจพบ โดยเทียบเคียงกับ MITRE ATT&CK stage ต่าง ๆ

4.2.11 ผู้ให้บริการต้องมีเครื่องมือที่แสดงข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียด อย่างน้อยดังนี้

4.2.11.1 ระบุประเภทของภัยคุกคาม

4.2.11.2 วัน-เวลา เริ่มต้นและสิ้นสุดของภัยคุกคาม

4.2.11.3 ระบุต้นทาง (Attacker) ปลายทาง (Target)

4.2.11.4 ระบุระดับความรุนแรง (Severity)

4.2.11.5 รายละเอียดเหตุการณ์และพฤติกรรม

4.2.11.6 ระบุรายละเอียดของช่องโหว่ (Vulnerability) ที่พบในเครื่องปลายทาง

4.2.12 ระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ที่นำมาให้บริการต้องเป็น Overall Leader เช่น IDC, Gartner, Forrester หรือ 2020 Kuppinger Cole Leadership Compass for SOAR เป็นต้น

4.2.13 ผู้ให้บริการต้องเสนอสิทธิ์ในการใช้งานระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ที่สามารถรองรับผู้ใช้งานระดับ Security Analyst ได้ไม่น้อยกว่า 2 ผู้ใช้งาน สำหรับเจ้าหน้าที่ กบข. และสามารถรองรับการสร้าง Workflow ได้ไม่จำกัด โดยไม่มีค่าใช้จ่ายเพิ่มเติมในส่วนของสิทธิ์การใช้งาน

4.2.14 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยในการทำ Accelerate Response โดยรองรับการทำงานร่วมกับระบบต่าง ๆ ดังนี้ได้เป็นอย่างน้อย

4.2.14.1 Security Information and Event Management (SIEM)

4.2.14.2 Endpoint Detection and Response (EDR)

4.2.14.3 Extended Detection and Response (XDR)

4.2.14.4 Firewall

4.2.14.5 Email Server

4.2.14.6 Active Directory

4.2.15 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยให้ทีมผู้ดูแลระบบต่าง ๆ ทำงานร่วมกัน ในลักษณะเชื่อมโยงข้อมูลการสนทนาที่เกี่ยวข้องกับ Incident รวมทั้งเก็บข้อมูลเกี่ยวกับ Incident, Log การทำงานของ Workflow/Playbook ต่าง ๆ

4.2.16 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยสร้าง Work Plan หรือ Workflow หรือ Playbook และสามารถทำ Sub Playbook ได้ โดยมีความสามารถอย่างน้อยดังนี้

4.2.16.1 การ Enrichment ข้อมูลร่วมกับ ข้อมูลที่ได้จาก Threat Intelligence Management หรือ Threat Intelligence Platform

4.2.16.2 การ Enrichment ข้อมูลร่วมกับระบบงานภายนอก เช่น Active Directory

4.2.16.3 สามารถสั่งการไปยัง Protection Tools เช่น Firewall หรือ IPS หรือ Endpoint security ได้

4.2.17 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยในการทำ Case Management เพื่อบริหารจัดการ Incident ต่าง ๆ ที่เกิดขึ้น เช่น กำหนดระยะเวลาในการตอบสนองต่อ Incident type ประเภทต่าง ๆ ได้ รวมถึงแสดง ผลการทำงานในภาพรวม ลักษณะ SLA Dashboard ได้ หรือนำเสนอระบบอื่น ๆ เพิ่มเติมเพื่อรองรับการทำงานลักษณะดังกล่าว

4.2.18 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยในการบริหารจัดการกับความรับผิดชอบงาน (Shift Management) ของผู้ดูแลระบบความปลอดภัย และสามารถส่ง Incident ให้กับผู้ดูแลระบบความปลอดภัยตามกะความรับผิดชอบงาน หรือภาระงาน (load) ได้

4.2.19 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยในการทำงานร่วมกันกับอุปกรณ์ความปลอดภัยที่มีอยู่ของ กบข. เช่น SIEM และ Endpoint Security ได้

4.2.20 ผู้ให้บริการต้องมีเครื่องมือที่ช่วยในการทำงานร่วมกับระบบรักษาความปลอดภัยเครือข่าย (Firewall) ที่มีอยู่เดิมของ กบข. ได้เป็นอย่างน้อย ดังนี้ เช่น ทำการ Block IP Address และทำการ Block URL ได้โดยอัตโนมัติ

4.2.21 ผู้ให้บริการต้องมีเครื่องมือที่มีระบบ Machine Learning เพื่อช่วยงาน Security Operation Center โดยมีความสามารถอย่างน้อย ดังนี้

4.2.21.1 ระบบแนะนำเลือกบุคลากรที่เหมาะสมสำหรับรับผิดชอบเป็น Owner ดูแลเหตุการณ์ที่เกิดขึ้น (Incident Owner Recommendations)

4.2.21.2 ระบบแนะนำและเชิญบุคลากรในทีมงานที่มีความสามารถมาร่วมแก้ไขปัญหา (Security Expert Suggestions)

4.2.21.3 ระบบให้คำแนะนำ Command ที่เหมาะสมในการใช้งานให้กับทางบุคลากร (Commonly Used Security Commands)

4.2.21.4 ระบบแสดง ให้เห็นภาพรวมเหตุการณ์ที่เกี่ยวข้องกัน (Visualizing Related Incidents)

4.2.22 ผู้ให้บริการต้องแสดงหลักฐานการมีสิทธิ์เสนอราคาสำหรับโครงการนี้ โดยต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากบริษัทเจ้าของผลิตภัณฑ์

4.2.23 ผู้ให้บริการต้องดำเนินการจัดฝึกอบรมให้ความรู้ด้านการใช้งานระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ให้กับบุคลากรของ กบข. จำนวนไม่น้อยกว่า 4 คน

5. การรับประกันความชำรุดบกพร่อง

5.1 ผู้ให้บริการต้องรับประกันความชำรุดบกพร่องของพัสดุที่ขอจ้างตลอดระยะเวลาตามพัสดุ ในระหว่างระยะเวลาการรับประกันดังกล่าว หากเกิดความชำรุดบกพร่องแก่งานที่ผู้ขายส่งมอบให้แก่ กบข. ตาม TOR นี้ หรือผู้ขายละเว้นการดำเนินการตาม TOR นี้ ไม่ว่าในส่วนหนึ่งส่วนใดหรือทั้งหมด ผู้ขายต้องเสนอแนวทางแก้ไขความชำรุดบกพร่องที่เกิดขึ้นให้ถูกต้องเป็นไปตามข้อกำหนดของ TOR ภายในระยะเวลา 1 วัน หรือตามที่ตกลงกัน โดย กบข. ไม่ต้องเสียค่าใช้จ่ายใด ๆ เพิ่มเติม

5.2 ผู้ให้บริการต้องให้คำปรึกษาด้านเทคนิคแก่ กบข. หรือเจ้าหน้าที่ผู้รับผิดชอบของ กบข. ผ่านอีเมล์และโทรศัพท์ได้ทุกวัน 24 ชั่วโมง ตลอดระยะเวลาสัญญา

6. หลักฐานการยื่นข้อเสนอ

ผู้ยื่นข้อเสนอจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมการเสนอราคาโดยแยกเป็น 2 ส่วน ดังต่อไปนี้

6.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีผู้ยื่นข้อเสนอเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคลที่มีระยะเวลาไม่เกิน 90 วัน นับถึงวันที่ยื่นข้อเสนอ บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคลที่มีระยะเวลาไม่เกิน 90 วัน นับถึงวันที่ยื่นข้อเสนอ หนังสือบริคณห์สนธิ บัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม(ถ้ามี) บัญชีผู้ถือหุ้นรายใหญ่ (ถ้ามี) พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาหรือคณะบุคคลที่ไม่ใช่นิติบุคคลให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน หรือสำเนาหนังสือเดินทางของผู้เป็นหุ้นส่วนที่มิได้ถือสัญชาติไทย พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้ยื่นข้อเสนอเป็นผู้ยื่นข้อเสนอร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า และเอกสารตามที่ระบุไว้ใน (1) หรือ (2) ของผู้ร่วมค้า แล้วแต่กรณี

(4) เอกสารเพิ่มเติมอื่น ๆ ได้แก่ สำเนาใบทะเบียนพาณิชย์ สำเนาทะเบียนภาษีมูลค่าเพิ่ม พร้อมทั้งรับรองสำเนาถูกต้อง

6.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีที่ผู้ยื่นข้อเสนอมอบอำนาจให้บุคคลอื่นกระทำการแทนให้แนบหนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมาย จะต้องระบุในหนังสือมอบอำนาจให้ชัดเจนว่ามีอำนาจในการเสนอราคาแทนหรือทำการในเรื่องใด โดยมีหลักฐานแสดงตัวตนของผู้มอบอำนาจและผู้รับมอบอำนาจ (แนบสำเนาบัตรประจำตัวประชาชนผู้มอบอำนาจและผู้รับมอบอำนาจพร้อมรับรองสำเนาถูกต้อง) ทั้งนี้ หากผู้รับมอบอำนาจเป็นบุคคลธรรมดาต้องเป็นผู้ที่บรรลุนิติภาวะตามกฎหมายแล้วเท่านั้น

(2) แคตตาล็อกและ/หรือแบบรูปรายการรายละเอียดคุณลักษณะเฉพาะ (ถ้ามี)

(3) ผู้ยื่นข้อเสนอต้องจัดทำตารางเปรียบเทียบคุณสมบัติของผู้ยื่นข้อเสนอราคา รายละเอียดคุณลักษณะเฉพาะที่ กบข. ต้องการ (ขอบเขตของงานที่ว่าจ้าง) และการรับประกันการชำรุดบกพร่อง ตาม TOR ข้อ 3 ข้อ 4 และข้อ 5 นี้ กับข้อเสนอของผู้ยื่นข้อเสนอ ซึ่งคุณลักษณะเฉพาะ (ขอบเขตของงานที่ว่าจ้าง) จะต้องระบุหัวข้อให้ถูกต้องตรงกันกับเอกสารหรือแคตตาล็อกที่เสนอโดยให้จัดทำในรูปแบบดังต่อไปนี้

ลำดับ	ข้อกำหนดตาม TOR	ความสอดคล้อง	รายละเอียดข้อเสนอ	เอกสารอ้างอิง
	▪ คัดลอกคุณสมบัติของผู้ยื่นข้อเสนอ <u>ตามที่กำหนดใน TOR ข้อ 3</u> ▪ คัดลอกข้อกำหนดรายละเอียดคุณลักษณะเฉพาะของงาน <u>(ขอบเขตของงานที่ว่าจ้าง)</u> ตามที่กำหนดใน TOR <u>ข้อ 4</u>	▪ ตรงหรือดีกว่าข้อกำหนดตาม TOR	▪ ระบุคุณสมบัติผู้ยื่นข้อเสนอ ▪ ระบุรายการและรายละเอียดคุณลักษณะเฉพาะของพัสดุที่เสนอมาให้พิจารณา	▪ ระบุเลขหน้าของเอกสารอ้างอิงหรือแคตตาล็อก

	▪ <u>การรับประกันการชำรุดบกพร่อง ตามที่กำหนดใน TOR ข้อ 5</u>			

(4) สำเนาใบขึ้นทะเบียนผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) (ถ้ามี)

(5) ผู้ยื่นข้อเสนอต้องจัดส่งเอกสารดังต่อไปนี้เพื่อประกอบการพิจารณาคัดเลือก

(1) เอกสารรายละเอียดของผู้ยื่นข้อเสนอ (Company Profile) เช่น ประวัติ/ข้อมูลบริษัท สินค้าและบริการ จำนวนพนักงาน เป็นต้น

(2) เอกสารอธิบายประสบการณ์ของผู้เสนอบริการ ที่มีลักษณะคล้ายกับงานตาม TOR ฉบับนี้ เช่น รายชื่อลูกค้าบริษัท (Site Reference) และข้อมูลโครงการ (หากสามารถเปิดเผยได้) (ถ้ามี)

(3) รายละเอียดด้านการบริหารการเฝ้าระวังภัยคุกคามทางไซเบอร์พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) (Project Management)

(4) รายละเอียดด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ตามที่กำหนดไว้ใน TOR ฉบับนี้

(5) ข้อมูลบุคลากรของผู้ยื่นข้อสนอที่นำมาทำงานให้แก่ กบข. (คุณวุฒิและประสบการณ์)

(6) รายละเอียดการบริการและความพร้อมให้บริการ (Service Availability)

7. การเสนอราคา

7.1 ผู้ยื่นข้อเสนอต้องยื่นข้อเสนอและเสนอราคาโดยไม่มีเงื่อนไขใด ๆ ทั้งสิ้น

7.2 ราคาที่เสนอจะต้องเป็นราคาที่รวมภาษีมูลค่าเพิ่ม ภาษีอื่น (ถ้ามี) รวมค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

7.3 ผู้ยื่นข้อเสนอต้องยืนราคาเป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่วันที่เสนอราคา โดยภายในกำหนดยืนราคา ผู้ยื่นข้อเสนอจะต้องรับผิดชอบราคาที่ตนเสนอไว้และถอนการเสนอราคามิได้

7.4 ผู้ยื่นข้อเสนอจะต้องดำเนินการตามข้อ 4.1 ให้แล้วเสร็จภายในวันที่ 31 กรกฎาคม 2565 และดำเนินการให้บริการและรับประกันตาม ข้อ 4.2 (ตั้งแต่วันที่ 1 สิงหาคม 2565 จนถึงวันที่ 31 กรกฎาคม 2567)

7.5 กรณีงานจัดจ้างที่ประกอบด้วยพัสดุหลายประเภทในโครงการเดียวกัน ผู้เสนอราคาต้องแยกราคาต่อหน่วยของพัสดุแต่ละประเภท (cost breakdown) ให้ชัดเจน (ถ้ามี)

8. หลักเกณฑ์และสิทธิในการพิจารณา

การพิจารณาผลการยื่นข้อเสนอครั้งนี้ กบข. จะพิจารณาตัดสินโดยใช้หลักเกณฑ์คะแนนรวมด้านคุณภาพและด้านราคาสูงที่สุด (Price Performance) ในการพิจารณาผู้ชนะการยื่นข้อเสนอ กบข. จะพิจารณาโดยให้คะแนนตามปัจจัยหลักและน้ำหนักที่กำหนด ดังต่อไปนี้

(1) ราคาที่ยื่นข้อเสนอ (Price) กำหนดน้ำหนักเท่ากับร้อยละ 30

(2) ข้อเสนอด้านเทคนิค กำหนดน้ำหนักเท่ากับร้อยละ 70

ข้อพิจารณา	คะแนนเต็ม (100 คะแนน)
1. ราคาที่ยื่นข้อเสนอ (price)	30 คะแนน
2. ข้อเสนอด้านเทคนิค โดยคำนึงถึงความเชื่อมโยง ลักษณะงาน และประสบการณ์ที่มีลักษณะใกล้เคียงกับการจัดจ้างนี้ เป็นสำคัญ 2.1 ผลงาน และความมั่นคงของผู้ยื่นข้อเสนอ (ร้อยละ 10) เช่น - รายละเอียดของผู้ยื่นข้อเสนอ (Company Profile) - ข้อมูลโครงการและหน่วยงานที่ผู้ยื่นข้อเสนอเคยรับทำงานให้ (Site Reference) ที่มีลักษณะคล้ายกับงานตาม TOR 2.2 รายละเอียดด้านการบริหารการเฝ้าระวังภัยคุกคามทางไซเบอร์พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) (Project Management) ที่ดำเนินงาน (ร้อยละ 10) เช่น - รายละเอียดการบริหารและวิธีการปฏิบัติงานด้านคุณภาพ และแผนการดำเนินงาน - รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่เพื่อดำเนินการตามแผนงาน	70 คะแนน

ข้อพิจารณา	คะแนนเต็ม (100 คะแนน)
2.3 รายละเอียดด้านการเฝ้าระวังภัยคุกคามทางไซเบอร์พร้อมระบบบริหารจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ที่ดำเนินงาน (ร้อยละ 25) เช่น - รายละเอียดแสดงกระบวนการหรือเทคนิคการจัดการข้อมูลการจราจรคอมพิวเตอร์และการเฝ้าระวังตามมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของ กบข. - ตัวอย่างเอกสารรายงานบทสรุปผู้บริหาร รายงานประจำวัน (Daily Report), รายงานประจำเดือน (Monthly Report), รายงานสรุปรายไตรมาส หรือทุกรอบระยะเวลา 3 เดือน (Quarterly Report) 2.4 รายละเอียดของเจ้าหน้าที่ตามแผนงาน (ร้อยละ 15) เช่น - รายละเอียดการจัดเตรียมเจ้าหน้าที่ตามตำแหน่งหน้าที่เพื่อดำเนินการตามแผนงาน - รายละเอียดทีมงานผู้ให้บริการ ประวัติการศึกษาและประกาศนียบัตรบอกถึงระดับของความรู้และประสบการณ์ที่เกี่ยวข้อง เช่น SANS Managing Security Operations หรือ SANS Blue Team Fundamentals หรือ CompTIA Cyber Security Analyst เป็นต้น 2.5 รายละเอียดการบริการและความพร้อมให้บริการ (Service Availability) (ร้อยละ 10) เช่น - เอกสารรายละเอียดบริการแจ้งเหตุขัดข้องระบบฯ - เอกสารที่แสดงถึงการกำหนดข้อตกลงความพร้อมให้บริการ (Service Availability)	

กบข. จะคัดเลือกยื่นข้อเสนอที่ได้คะแนนสูงที่สุดอันดับแรก เข้ารับการทดสอบข้อเสนอทางด้านเทคนิค (POC) โดย กบข. จะเป็นผู้กำหนดหัวข้อการทดสอบ โดยอ้างอิงเอกสารรายละเอียดการทดสอบข้อเสนอทางด้านเทคนิค (POC) (เอกสารแนบท้าย) ในกรณีที่ผู้ยื่นข้อเสนอทดสอบไม่ผ่าน หรือปฏิเสธการทดสอบ หรือปฏิเสธการลงนามยินยอมไม่เปิดเผยความลับ (NDA) จะแจ้งผู้ให้บริการลำดับถัดไปเข้ามาทดสอบ

กบข. สงวนสิทธิ์ที่จะไม่รับราคาต่ำสุด หรือราคาหนึ่งราคาใด หรือราคาที่เสนอทั้งหมดก็ได้ หรืออาจจะยกเลิกการจ้างในครั้งนี้ ทั้งนี้เพื่อประโยชน์ของ กบข. เป็นสำคัญ และให้ถือว่าคำตัดสินของ กบข. ถือเป็นที่สุด ผู้ให้บริการจะเรียกร้องค่าเสียหายใด ๆ มิได้ และ กบข. สงวนสิทธิ์ในการโต้แย้ง

9. การทำสัญญาจ้าง

ผู้ชนะการคัดเลือกจะต้องทำสัญญาจ้างตามแบบที่ กบข. กำหนดภายใน 15 วัน นัดถัดจากวันที่ได้รับแจ้งจาก กบข. และจะต้องวางหลักประกันสัญญาเป็นเงินเท่ากับร้อยละ 5 ของราคาค่าจ้าง

10. ค่าจ้างและการจ่ายเงิน

กบข. จะจ่ายค่าจ้างซึ่งได้รวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว ให้แก่ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกให้เป็นผู้รับจ้างภายใน 30 วัน เมื่อผู้รับจ้างได้ปฏิบัติงานถูกต้องและครบถ้วนตามสัญญาจ้างหรือข้อตกลง และ กบข. ได้ตรวจรับมอบงานจ้างเรียบร้อยแล้วพร้อมทั้ง กบข. ได้รับหนังสือเรียกเก็บเงินจากผู้รับจ้าง โดยแบ่งการจ่ายเงินตามรายละเอียดข้อ 4.1 และ 4.2 ดังต่อไปนี้

- งวดที่ 1 ชำระในอัตราร้อยละ 4 ของมูลค่าในสัญญา หลังจากที่ส่งมอบรายงานการการเตรียมการก่อนการให้บริการ (Implementation) ตามรายละเอียดข้อ 4.1 และส่งมอบรายงานการเฝ้าระวังภัยคุกคามทางไซเบอร์ประจำเดือนสิงหาคม 2565 ภายในวันที่ 5 ของเดือนถัดไป ตามรายละเอียดข้อ 4.2
- งวดที่ 2 - 23 ชำระในอัตราร้อยละ 4 ของมูลค่าในสัญญา หลังจากที่ส่งมอบรายงานการเฝ้าระวังภัยคุกคามทางไซเบอร์ประจำเดือนกันยายน 2565 จนถึง มิถุนายน 2567 ภายในวันที่ 5 ของเดือนถัดไป ตามรายละเอียดข้อ 4.2 เรียบร้อยแล้ว
- งวดที่ 24 ชำระในส่วนที่เหลือทั้งหมดของมูลค่าในสัญญา หลังจากที่ส่งมอบรายงานการเฝ้าระวังภัยคุกคามทางไซเบอร์ประจำเดือนกรกฎาคม 2567 ภายในวันที่ 5 ของเดือนถัดไป ตามรายละเอียดข้อ 4.2 เรียบร้อยแล้ว

ผู้รับจ้างจะต้องทำข้อมูลเปรียบเทียบงานที่ส่งมอบแต่ละงวดงานกับงานตามที่สัญญากำหนดว่าส่งมอบได้ครบถ้วนหรือไม่ โดยให้จัดทำในรูปแบบ ดังต่อไปนี้

ลำดับ	ข้อกำหนดตาม TOR	ความสอดคล้อง	รายละเอียดของงานที่ส่งมอบ	เอกสารอ้างอิง
	▪ คัดลอกข้อกำหนดรายละเอียดคุณลักษณะเฉพาะของงานตามที่กำหนดใน TOR ▪ คัดลอกการรับประกัน	▪ ตรงหรือดีกว่าข้อกำหนดตาม TOR	▪ ระบุรายการและรายละเอียดคุณลักษณะเฉพาะของงานที่ส่งมอบ ▪ ระบุรายละเอียดการรับประกันงานที่ส่งมอบ	▪ ระบุเลขหน้าของเอกสารอ้างอิงหรือแคตตาล็อก

11. อัตราค่าปรับ

ค่าปรับตามสัญญาจ้างหรือข้อตกลงจ้างเป็นหนังสือจะกำหนดไว้ดังต่อไปนี้

11.1 กรณีที่ผู้รับจ้างนำงานที่รับจ้างไปจ้างช่วงให้ผู้อื่นทำอีกทอดหนึ่งโดยไม่ได้รับอนุญาตจาก กบข. จะกำหนดค่าปรับสำหรับการฝ่าฝืนดังกล่าวเป็นจำนวนร้อยละ 10 ของวงเงินของงานจ้างช่วงนั้น

11.2 กรณีที่ผู้รับจ้างปฏิบัติผิดสัญญาจ้างนอกเหนือจากข้อ 10.1 จะกำหนดค่าปรับเป็นรายวันในอัตราร้อยละ 0.1 ของราคาค่าจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100 บาท

12. วงเงินในการจัดจ้าง

วงเงินในการจัดจ้างครั้งนี้เป็นเงิน 12,320,000.00 บาท (สิบสองล้านสามแสนสองหมื่นบาทถ้วน) ซึ่งรวมภาษีมูลค่าเพิ่ม ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงด้วยแล้ว

13. ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ

13.1 ผู้ยื่นข้อเสนอซึ่ง กบข. ได้คัดเลือกแล้ว ไม่ไปทำสัญญาหรือข้อตกลงซื้อเป็นหนังสือภายในเวลาที่กำหนด กบข. จะริบหลักประกันการยื่นข้อเสนอ (ถ้ามี) หรือเรียกร้องจากผู้ออกหนังสือค้ำประกันการยื่นเสนอราคาทันที และอาจพิจารณาเรียกร้องให้ชดใช้ความเสียหายอื่น (ถ้ามี) รวมทั้งจะพิจารณาให้เป็นผู้ทิ้งงานตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ

13.2 ข้อมูลที่เป็นความลับ

"ข้อมูลที่เป็นความลับ" หมายความถึง ข้อมูลใด ๆ ที่ กบข. หรือพนักงานของ กบข. ได้เปิดเผยแก่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย โดย กบข. หรือพนักงานของ กบข. มีความประสงค์ให้ผู้ขายหรือลูกจ้างหรือผู้แทนของผู้ขาย เก็บรักษาข้อมูลดังกล่าวไว้เป็นความลับ โดยข้อมูลดังกล่าวเกี่ยวข้องกับข้อมูลที่ กบข. จัดเก็บหรือครอบครองอยู่ รวมถึงข้อมูลของ กบข. ที่เป็นกระบวนการ ขั้นตอนวิธี โปรแกรมคอมพิวเตอร์ โครงสร้างด้านระบบ โครงสร้างฐานข้อมูล ข้อมูลด้านเครือข่าย ข้อมูลสูตร เทคนิค ข้อมูลผลิตภัณฑ์ ข้อมูลการทดลอง ข้อมูลเกี่ยวกับการบริหาร และแผนงาน

13.3 การเปิดเผยและการรักษาข้อมูลที่เป็นความลับ

(1) ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ตกลงและรับทราบว่าข้อมูลที่เป็นความลับที่เปิดเผยภายใต้สัญญาจ้างถือเป็นและจะยังคงเป็นทรัพย์สินและทรัพย์สินทางปัญญา (ถ้ามี) ของ กบข.

(2) ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ตกลงว่าจะเก็บรักษาข้อมูลที่เป็นความลับที่ กบข. หรือพนักงานของ กบข. ได้เปิดเผยให้แก่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ภายใต้สัญญาจ้างตลอดระยะเวลาการปฏิบัติงานของผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ตามสัญญาซื้อขาย และเป็นระยะเวลา 1 (หนึ่ง) ปี นับแต่วันที่สัญญาจ้างดังกล่าวสิ้นสุดลง โดยผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ตกลงที่จะดำเนินการ ดังต่อไปนี้

(ก) รักษาข้อมูลที่เป็นความลับที่ได้รับมาอย่างเคร่งครัด และไม่เปิดเผยข้อมูลที่เป็นความลับ ไม่ว่าทั้งหมดหรือแต่บางส่วนให้แก่บุคคลใดทราบ เว้นแต่จะเป็นการเปิดเผยข้อมูลที่เป็นความลับให้แก่ลูกจ้างหรือผู้แทนของผู้ขายที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลที่เป็นความลับนั้นเท่านั้น และผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย จะต้องจัดให้ลูกจ้างหรือผู้แทนของตนได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับด้วย

(ข) ใช้ข้อมูลที่เป็นความลับเพียงเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ในสัญญาจ้างเท่านั้น

(ค) เก็บรักษาเอกสาร บันทึก หรือวัตถุอื่นใดที่บรรจุข้อมูลที่เป็นความลับที่ได้รับมาไว้ในสถานที่ที่ปลอดภัยที่บุคคลทั่วไปไม่สามารถเข้าถึงได้โดยง่าย และรักษาข้อมูลที่เป็นความลับที่ได้รับมาในลักษณะและระดับเดียวกันกับการรักษาข้อมูลที่เป็นความลับของตนเอง แต่ทั้งนี้ จะต้องไม่น้อยกว่าระดับที่วิญญูชนพึงรักษาข้อมูลที่เป็นความลับของตนเอง

(ง) ไม่ทำซ้ำซึ่งข้อมูลที่เป็นความลับแม้เพียงส่วนหนึ่งส่วนใดหรือทั้งหมด เว้นแต่การทำซ้ำเพื่อการใช้ข้อมูลที่เป็นความลับให้บรรลุผลตามวัตถุประสงค์ที่กำหนดไว้สัญญาจ้างเท่านั้น และไม่ทำวิศวกรรมย้อนกลับ หรือ ถอดรหัสข้อมูลที่เป็นความลับ ต้นแบบ หรือสิ่งอื่นใดที่บรรจุข้อมูลที่เป็นความลับรวมทั้งไม่เคลื่อนย้าย พิมพ์ทับ หรือทำให้เสียรูปซึ่งสัญลักษณ์ที่แสดงเครื่องหมายสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า ตราสัญลักษณ์ และเครื่องหมายอื่นใดที่แสดงกรรมสิทธิ์ของต้นแบบหรือสำเนาของข้อมูลที่เป็นความลับที่ได้รับมาจากกบข. หรือพนักงานของ กบข.

13.4 ข้อยกเว้นในการรักษาข้อมูลที่เป็นความลับ

หน้าที่ในการรักษาข้อมูลที่เป็นความลับดังกล่าวจะไม่ใช้บังคับกับผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย หากผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย สามารถแสดงพยานหลักฐานได้ว่า

(1) ข้อมูลดังกล่าวเป็นข้อมูลที่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ได้รับทราบอยู่ก่อนที่ กบข. หรือพนักงานของ กบข. จะได้เปิดเผยข้อมูลนั้น

(2) ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ได้รับข้อมูลที่เป็นความลับจากบุคคลที่สามที่ไม่อยู่ภายใต้ข้อกำหนดในเรื่องการรักษาความลับหรือข้อจำกัดในเรื่องสิทธิการใช้ประโยชน์ข้อมูลที่เป็นความลับนั้น

(3) ข้อมูลดังกล่าวเป็นข้อมูลที่รู้กันโดยทั่วไปก่อนหรือขณะเวลาที่ กบข. หรือพนักงานของ กบข. เปิดเผยข้อมูลที่เป็นความลับแก่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย หรือเป็นข้อมูลที่เป็นความลับที่ได้เปิดเผยต่อสาธารณะหลังจากที่ กบข. หรือพนักงานของ กบข. ได้เปิดเผยข้อมูลที่เป็นความลับให้แก่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย

(4) กบข. หรือพนักงานของ กบข. ได้เปิดเผยข้อมูลที่เป็นความลับต่อบุคคลภายนอก โดยไม่มีข้อกำหนดให้บุคคลภายนอกต้องรักษาความลับของข้อมูล หรือไม่มีข้อจำกัดในการใช้ข้อมูลที่เป็นความลับดังกล่าว

(5) ข้อมูลดังกล่าวเป็นข้อมูลที่มาจากการพัฒนาโดยอิสระของผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย

(6) ข้อมูลดังกล่าวเป็นข้อมูลที่กำหนดให้ต้องเปิดเผยโดยกฎหมายหรือตามคำสั่งศาล ทั้งนี้ ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย จะต้องแจ้งเป็นหนังสือให้ กบข. หรือพนักงานของ กบข. ได้รับทราบถึงข้อกำหนดหรือคำสั่งดังกล่าวก่อนที่จะดำเนินการเปิดเผยข้อมูลดังกล่าว และในการเปิดเผยข้อมูลดังกล่าว ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย จะต้องดำเนินการตามขั้นตอนทางกฎหมายเพื่อขอให้คุ้มครองข้อมูลดังกล่าวไม่ให้ถูกเปิดเผยต่อสาธารณะด้วย

(7) ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ได้รับความยินยอมเป็นหนังสือจาก กบข. หรือพนักงานของ กบข. ก่อนเปิดเผยข้อมูลนั้น

13.5 วิธีปฏิบัติเมื่อสัญญาสิ้นสุดลง

เมื่อสัญญาจ้างสิ้นสุดลง ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย จะต้องส่งมอบข้อมูลที่เป็นความลับและสำเนาของข้อมูลที่เป็นความลับที่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ได้รับไว้ คืนให้แก่ กบข. หรือพนักงานของ กบข. ทั้งหมด หรือทำลายข้อมูลที่เป็นความลับที่ได้รับจาก กบข. หรือพนักงานของ กบข. ทั้งหมด และแจ้งยืนยันเป็นลายลักษณ์อักษรถึงการทำลายดังกล่าวให้ กบข. หรือพนักงานของ กบข. ทราบ ตลอดจนยุติการใช้ข้อมูลที่เป็นความลับและสิทธิใด ๆ ภายใต้สัญญาจ้างทันที ทั้งนี้ ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ยังคงมีหน้าที่รักษาความลับของข้อมูลที่ได้รับภายใต้สัญญาจ้างตามระยะเวลาที่กำหนดไว้ แม้สัญญาจ้างสิ้นสุดลงแล้ว

13.6 การชดใช้ค่าเสียหาย

(1) กรณีที่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ฝ่าฝืนข้อกำหนดตามสัญญาจ้าง และก่อให้เกิดความเสียหายแก่ กบข. ผู้ขายจะต้องชดใช้ค่าเสียหายที่เกิดขึ้นให้แก่ กบข.

(2) ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย รับทราบว่า การเปิดเผยหรือการใช้ข้อมูลที่เป็นความลับโดยฝ่าฝืนข้อกำหนดตามสัญญาจ้างอาจก่อให้เกิดความเสียหายแก่ กบข. เป็นจำนวนที่ไม่สามารถประเมินได้ ดังนั้นผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ยินยอมให้ กบข. ใช้สิทธิที่จะร้องขอต่อศาลเพื่อให้มีคำสั่งให้ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย หยุดการกระทำใด ๆ ที่เป็นการฝ่าฝืนข้อกำหนดตามสัญญานี้ และ/หรือใช้วิธีคุ้มครองชั่วคราวใด ๆ ตามที่ กบข. เห็นว่าเหมาะสมได้ โดยผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย จะเป็นผู้รับผิดชอบค่าใช้จ่ายต่าง ๆ ทั้งหมดในการดำเนินการดังกล่าว

(3) กรณีที่ กบข. สงสัยว่าผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ฝ่าฝืนข้อตกลงตามสัญญาจ้าง ผู้ขายจะต้องเป็นฝ่ายพิสูจน์ว่าผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขาย ไม่ได้ฝ่าฝืนข้อตกลงตามสัญญาจ้าง

13.7 ข้อกำหนดอื่น

(1) การที่ กบข. หรือพนักงานของ กบข. เปิดเผยข้อมูลที่เป็นความลับให้แก่ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขายตามสัญญาซื้อขาย ไม่ถือว่า กบข. ได้อนุญาตให้ผู้ขาย หรือลูกจ้างหรือผู้แทนของผู้ขายใช้ผลงานซึ่งมีสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า หรือข้อมูลทางการค้าอื่นของ กบข. เว้นแต่ กบข. จะมีหนังสือแสดงความตกลงเป็นอย่างอื่น

(2) กรณีที่ผู้ขายได้โอนกิจการ รวมกิจการ หรือควบกิจการ หรือดำเนินการอื่น ๆ ในลักษณะที่มีการเปลี่ยนแปลงอำนาจในการดำเนินกิจการ ผู้ขายจะต้องแจ้งให้ กบข. ทราบโดยไม่ชักช้า การที่ กบข. ทำสัญญาจ้างกับผู้ขาย ไม่มีผลผูกพัน กบข. ที่จะต้องเปิดเผยรายละเอียดของข้อมูลที่เป็นความลับภายใต้สัญญาจ้าง หรือที่จะต้องเข้าทำสัญญาอนุญาตให้ใช้สิทธิกับผู้ขายในการใช้ประโยชน์ข้อมูลที่เป็นความลับต่อไป

14. มาตรการป้องกันการทุจริตและประพฤติมิชอบ

ด้วย กบข. มีนโยบายต่อต้านการทุจริตและประพฤติมิชอบที่บั่นทอนเศรษฐกิจและสังคมของประเทศ กบข. ไม่ยอมรับการทุจริตและประพฤติมิชอบทุกรูปแบบ (Zero Tolerance) ไม่ว่าจะเป็นการกระทำโดยบุคลากรของ กบข. หรือบริษัทในเครือของ กบข. หรือบุคคลที่เกี่ยวข้องกับกิจการของ กบข. ซึ่งรวมถึงคู่ค้าของ กบข. ทุกราย นอกจากนี้ กบข. ยังยึดมั่นในการดำเนินธุรกิจอย่างมีจริยธรรม จรรยาบรรณ และรับผิดชอบต่อสังคมและผู้มีส่วนได้เสียทุกกลุ่มด้วย

กบข. จึงขอความร่วมมือจากผู้ยื่นข้อเสนอ หากพบเห็นการกระทำของบุคลากรของ กบข. หรือบริษัทในเครือของ กบข. หรือบุคคลที่เกี่ยวข้องกับกิจการของ กบข. หรือคู่ค้าของ กบข. รายใดที่มีการกระทำเข้าข่ายทุจริต ติดสินบน หรือเรียกรับเงิน ทรัพย์สินหรือประโยชน์อื่นใดที่ไม่เหมาะสม ไม่ว่าในรูปแบบใด ขอให้แจ้งโดยตรงไปยังบุคคลและที่อยู่ดังต่อไปนี้

"ประธานอนุกรรมการตรวจสอบ
ฝ่ายตรวจสอบภายใน กองทุนบำเหน็จบำนาญข้าราชการ
เลขที่ 990 อาคารอับดุลราฮิม เพลส ถนนพระราม 4
แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500"

15. ผู้จัดทำขอบเขตของงาน (Terms of Reference: TOR)

1. นายวัชรพงศ์ ชัยกิจ
2. นางสาวณัฐสุดา ศรีคล้าย

รายละเอียดการทดสอบข้อเสนอทางด้านเทคนิค (POC)

1. ผู้ให้บริการต้องจัดเตรียมสภาพแวดล้อม ระบบที่นำมาทดสอบข้อเสนอทางด้านเทคนิค (POC) ดังนี้
   1.1. ระบบบริหารการจัดการและตอบสนองต่อภัยคุกคามแบบอัตโนมัติ (Security Orchestration Automation and Response: SOAR) ที่จะนำมาใช้ในการให้บริการ
   1.2. ระบบจัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (Security Information and Event Management: SIEM) เป็นผลิตภัณฑ์ QRadar
   1.3. ระบบป้องกันและรักษาความปลอดภัยระบบเครือข่าย (Firewall) เป็นผลิตภัณฑ์ Fortinet
   1.4. ระบบตรวจสอบและตอบสนองต่อภัยคุกคาม (Next-Generation Antivirus + Endpoint Detection & Response) เป็นผลิตภัณฑ์ Carbon Black
   1.5. อีเมล เป็นผลิตภัณฑ์ Microsoft
   1.6. เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้เป็น Active Directory
   1.7. เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้เป็น Email Server
   1.8. เครื่องคอมพิวเตอร์ลูกข่ายที่มีการเชื่อมต่อกับเครื่องแม่ข่าย และติดตั้ง Agent ของ Carbon Black
2. ระยะเวลาในการทดสอบข้อเสนอทางด้านเทคนิค (POC)
   2.1. จัดเตรียมระบบก่อนการทดสอบ ระยะเวลา 2 วัน
   2.2. การทดสอบข้อเสนอทางด้านเทคนิค ระยะเวลา 1 วัน

หัวข้อ	ผลการทดสอบ	
	ผ่าน	ไม่ผ่าน
1. ทดสอบเชื่อมต่อกับระบบต่าง ๆ		
1.1 ระบบ SOAR ทำการเชื่อมต่อกับระบบ SIEM (QRadar)		
1.2 ระบบ SOAR ทำการเชื่อมต่อกับระบบ Firewall (Fortinet)		
1.3 ระบบ SOAR ทำการเชื่อมต่อกับระบบ Next-Gen AV + EDR (Carbon Black)		
1.4 ระบบ SOAR ทำการเชื่อมต่อกับ Active Directory		
1.5 ระบบ SOAR ทำการเชื่อมต่อกับ Email Server		
2. ทดสอบการทำงานร่วมกับระบบต่าง ๆ โดยจำลองสถานการณ์ เครื่องลูกข่ายพยายามเข้าถึง Malicious Website		
2.1 เครื่องลูกข่ายทำการเข้าถึง Malicious Website ผ่าน Firewall (Fortinet)		
2.2 Firewall (Fortinet) ทำการส่ง Log ไปที่ SIEM (QRadar)		
2.3 SOAR ทำการ Fetch Incident ที่เกิดขึ้นบน Offense ของ SIEM (QRadar)		

2.4 SOAR ทำการแจ้งเตือนผ่าน Email Server และส่งต่อไปยังอีเมล (O365)		
2.5 SOAR สั่งการให้ Firewall (Fortinet) ทำการ Block IP Address และ Block URL		
2.6 SOAR สั่งการให้ Next-Gen AV + EDR (Carbon Black) ทำการ Quarantine Device		
2.7 SOAR แจ้งเตือนไปยังผู้ดูแลระบบ ผ่าน Mobile Application หรือ E-Mail เพื่อให้ผู้ดูแลระบบตรวจสอบและตัดสินใจ (Approve / Reject) ในระหว่างกระบวนการทำงานของ Playbook ได้		