ร่างขอบเขตของงาน รายละเอียดคุณลักษณะเฉพาะ

การประกวดราคาซื้ออุปกรณ์และระบบรักษาความปลอดภัยเพิ่มประสิทธิภาพ ด้านความมั่นคงทางเครือข่าย (Network Security) จำนวน ๑๓ รายการ ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e - bidding)

จำนวน ๒๘ หน้า

<u>การเสนอแนะหรือวิจารณ์ร่างขอบเขตของงาน (Terms of- Reference : TOR)</u>

หากผู้ยื่นข้อเสนอประสงค์จะเสนอแนะหรือวิจารณ์ ร่างรายละเอียดขอบเขตของงาน (Terms of-Reference : TOR) รายละเอียดคุณลักษณะเฉพาะ ให้เสนอแนะ วิจารณ์ หรือมีความเห็นเป็นลายลักษณ์อักษร ผ่านทางจดหมายลงทะเบียนโดยเปิดเผยตัว ส่งมาที่ฝ่ายพัสดุ กลุ่มงานพัสดุ กองคลัง กรมการปกครอง อาคารธนาลงกรณ์ทาวเวอร์ ชั้นที่ ๑๙ แขวงบางบำหรุ เขตบางพลัด กรุงเทพมหานคร ๑๐๗๐๐ หรือทางอีเมล์ m03030001@dopa.go.th หรือสอบถามรายละเอียดได้ที่โทรศัพท์หมายเลข ๐ ๒๒๒๕ ๔๘๘๗, ๐๖๓ ๙๐๓ ๑๐๒๕ (กองคลัง) หรือ ๐ ๒๗๙๑ ๗๒๒๕ (สำนักบริหารการทะเบียน)

ร่าง

(Terms of Reference : TOR)

รายละเอียดคุณลักษณะเฉพาะของโครงการจัดหาอุปกรณ์และระบบรักษาความปลอดภัย เพิ่มประสิทธิภาพด้านความมั่นคงทางเครือข่าย (Network Security) ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

****

๑. ความเป็นมา

สำนักบริหารการทะเบียน กรมการปกครอง เป็นหน่วยงานหลักของประเทศที่มีระบบคอมพิวเตอร์แม่ข่ายที่ให้บริการงานประชาชนและบริการภาครัฐ ตลอดเวลา ๗ วัน ๒๔ ชั่วโมง โดยได้มีการดำเนินการให้พัฒนาระบบฐานข้อมูลของประเทศมาอย่างต่อเนื่องและได้ปฏิรูปการบริหารจัดการภาครัฐ เพื่อการขับเคลื่อนและบริหารประเทศสามารถบริหารจัดการได้อย่างมีประสิทธิภาพในโครงการการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ ทำให้เกิดการใช้ประโยชน์ข้อมูลขนาดใหญ่ในการบริการประชาชน ซึ่งสำนักบริหารการทะเบียน กรมการปกครอง ได้พัฒนาการบริการประชาชนให้เป็นไปตามความต้องการเฉพาะตัวบุคคลมากขึ้น พัฒนาโปรแกรมออนไลน์เพื่อให้ประชาชนสามารถเข้าถึงบริการภาครัฐได้สะดวกรวดเร็วยิ่งขึ้น ทำให้มีข้อมูลต่าง ๆ ไหลเวียนอยู่บนโลกออนไลน์ ปัจจุบันแนวโน้วของภัยคุกคามทางไซเบอร์ ยิ่งมีความรุนแรงและแพร่หลายมากขึ้น ประกอบกับได้มีการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ทั้งนี้ สำนักบริหารการทะเบียน กรมการปกครอง ถูกประกาศให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามประกาศคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมกำกับดูแล พ.ศ. ๒๕๖๔ จึงมีความจำเป็นอย่างยิ่งที่ต้องจัดหาอุปกรณ์และระบบรักษาความปลอดภัยเพิ่มประสิทธิภาพด้านความมั่นคงทางเครือข่าย (Network Security) และเสริมสร้างความรู้และศักยภาพของผู้ปฏิบัติงานหรือผู้ที่เกี่ยวข้องกับการเฝ้าระวังด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศได้เรียนรู้และฝึกปฏิบัติอย่างเข้มข้น โดยมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ด้านบริการภาครัฐที่สำคัญ สำนักบริหารการทะเบียน กรมการปกครอง (BORA CIRT) เพื่อประสานงาน เฝ้าระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ด้านบริการภาครัฐที่สำคัญ รวมทั้งต้องมีการจัดทำรายงานต่าง ๆ จากการเฝ้าระวัง การวิเคราะห์ข้อมูลการจราจรทางคอมพิวเตอร์ (Log) โดยใช้ซอฟต์แวร์เชิงพาณิชย์ และการจัดเก็บหลักฐานเหตุการณ์ด้านความมั่นคงปลอดภัยเพื่อตรวจสอบช่องทางการเข้าถึงเครือข่ายและระบบสารสนเทศต่าง ๆ ที่ผิดปกติ เพื่อตอบสนองต่อเหตุการณ์และแก้ปัญหาการบุกรุกระบบอย่างรวดเร็วและมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยของข้อมูลต่าง ๆ ที่อยู่บนโลกออนไลน์

๒.๒ เพื่อเพิ่มประสิทธิภาพให้กับโครงข่ายระบบสารสนเทศ ของสำนักบริหารการทะเบียน กรมการปกครอง ให้มีความเสถียรภาพมากขึ้น

๒.๓ เพื่อเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามทางไซเบอร์

๓. คุณสมบัติของผู้ยื่นเสนอราคา

๓.๑ มีความสามารถตามกฎหมาย

๓.๒ ไม่เป็นบุคคลล้มละลาย

๓.๓ ไม่อยู่ระหว่างเลิกกิจการ

๓.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

๓.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลางซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๓.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๓.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๓.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมการปกครอง ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๓.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์ความคุ้มกันเช่นว่านั้น

๓.๑๐ ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอ ผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

๓.๑๑ ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e - GP) ของกรมบัญชีกลาง

๓.๑๒ ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(๑) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งได้จดทะเบียนเกินกว่า ๑ ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ของ ๑ ปีสุดท้ายก่อนวันยื่นข้อเสนอ ซึ่งจะต้องแสดงค่าเป็นบวก

(๒) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย/กฎหมายต่างประเทศ ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียนโดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า ๒๐ ล้านบาท

(๓) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน ๕๐๐,๐๐๐ บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดาถือสัญชาติไทย/บุคคลธรรมดาที่มิได้ถือสัญชาติไทย จะต้องยื่นหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วันก่อนวันยื่นข้อเสนอ และให้พิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน ๙๐ วันก่อนวันยื่นข้อเสนอโดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการ ที่ยื่นข้อเสนอในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดง หนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(๔) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะยื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อที่ธนาคารภายในประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาต

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

ให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ หรือเป็นสินเชื่อที่ธนาคารต่างประเทศหรือบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารกลางต่างประเทศนั้น ตามรายชื่อบริษัทเงินทุนที่ธนาคารกลางของประเทศนั้นแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอ นับถึงวันยื่นข้อเสนอไม่เกิน ๙๐ วัน โดยต้องมีวงเงินสินเชื่อจากธนาคารไม่น้อยกว่า ๑ ใน ๔ ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอในแต่ละครั้ง ทั้งนี้ สำหรับธนาคารภายในประเทศหนังสือรับรองวงเงินสินเชื่อให้เป็นไปตามแบบที่กำหนด

(๕) กรณีตาม (๑) - (๔) ยกเว้นสำหรับกรณีดังต่อไปนี้

(๕.๑) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(๕.๒) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระบัญญัติล้มละลาย (ฉบับที่ ๑๐) พ.ศ. ๒๕๖๑

(๖) กรณีตามข้อ (๒) ข้อ (๓) และข้อ (๔) มูลค่าจะต้องเป็นไปตามอัตราแลกเปลี่ยนเงินตราตามประกาศที่ธนาคารแห่งประเทศไทยกำหนด ในช่วงระหว่างวันที่เผยแพร่ประกาศและเอกสารเชิญชวนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (e – GP) หรือมีหนังสือเชิญชวน จนถึงวันเสนอราคา

๔ คุณสมบัติผู้เสนอราคา (เพิ่มเติม)

๔.๑ ผู้ประสงค์จะเสนอราคาต้องได้ใบรับรองตามมาตรฐาน ISO ๙๐๐๑ : ๒๐๑๕ ในเรื่องคุณภาพการออกแบบ พัฒนา ติดตั้ง ซ่อมบำรุง ระบบคอมพิวเตอร์และเครือข่ายระบบคอมพิวเตอร์ ศูนย์รวม และระบบปฏิบัติการ โดยจะต้องแสดงสำเนาหลักฐานรับรองที่ไม่หมดอายุ

๔.๒ ผู้ยื่นข้อเสนอต้องมีผลงานการจำหน่ายระบบคอมพิวเตอร์ฮาร์ดแวร์และซอฟต์แวร์พร้อมการติดตั้งให้แก่หน่วยงานเป็นสัญญาเดียวโดยมีมูลค่าผลงานในวงเงินไม่น้อยกว่า ๔๙,๐๐๐,๐๐๐ บาท (สี่สิบเก้าล้านบาทถ้วน) ภายในสัญญาเดียว อย่างน้อย ๑ ผลงาน แนบมาพร้อมกับการยื่นข้อเสนอ ผลงานที่ผู้ยื่นข้อเสนอจะต้องใช้งานได้ในปัจจุบันเป็นที่ยอมรับในมาตรฐานทั่วไปและปฏิบัติถูกต้องตามเงื่อนไขแห่งสัญญานั้นทุกประการและเป็นผลงานที่เป็นคู่สัญญาโดยตรงกับหน่วยงานราชการพร้อมแนบสำเนาหนังสือรับรองผลงานและสำเนาสัญญามาแสดง โดยผลงานดังกล่าวกรมการปกครอง หรือคณะกรรมการพิจารณาผล มีสิทธิเข้าไปดูสถานที่หรือตรวจสอบผลงานนั้น เพื่อประกอบการพิจารณาคัดเลือกผู้ยื่นข้อเสนอที่มีคุณภาพและคุณสมบัติที่เป็นประโยชน์ต่อทางราชการ

๔.๓ ผู้ยื่นข้อเสนอต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายอุปกรณ์และระบบซอฟต์แวร์ที่เสนอจากผู้ผลิตหรือตัวแทนจำหน่ายในประเทศไทยที่ถูกต้องตามกฎหมาย โดยจะต้องแสดงเอกสารที่ได้รับการแต่งตั้งให้เป็นตัวแทนจำหน่ายและหนังสือรับรองมีอายุไม่เกิน ๓๐ วัน นับจากวันที่ออกจนถึงวันที่ยื่นเอกสารเสนอราคาและต้องระบุโครงการที่ประกาศฯด้วยโดยให้แนบเอกสารขณะเข้าเสนอราคา ตามรายการอุปกรณ์ดังต่อไปนี้

๔.๓.๑ อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC : Network Access Control)

๔.๓.๒ ซอฟต์แวร์ระบบป้องกันและควบคุมการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Protection)

๔.๓.๓ อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร E-mail (E-mail Security Gateway)

๔.๓.๔ ระบบป้องกันการเข้าถึงข้อมูลระดับสูง (Privileged Account Security Management)

๔.๓.๕ ระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM)

๔.๓.๖ ระบบตรวจจับภัยคุกคามและตอบสนองต่อระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response : NDR)

๔.๓.๗ อุปกรณ์วิเคราะห์ข้อมูลระบบเครือข่ายและออกรายงานแบบรวมศูนย์

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

๕. ขอบเขตงาน

๕.๑ ผู้ประสงค์จะเสนอราคาต้องดำเนินการจัดหาอุปกรณ์และระบบรักษาความปลอดภัยเพิ่มประสิทธิภาพด้านความมั่นคงทางเครือข่าย (Network Security) พร้อมติดตั้ง ให้เป็นไปตามวัตถุประสงค์ของโครงการ โดยมีรายละเอียดคุณลักษณะเฉพาะระบบคอมพิวเตอร์ ดังนี้

๕.๑.๑ ระบบคอมพิวเตอร์ฮาร์ดแวร์

๕.๑.๑.๑ เครื่องคอมพิวเตอร์แม่ข่ายและซอฟต์แวร์สำหรับให้บริการเครื่องคอมพิวเตอร์แบบเสมือน จำนวน ๘ หน่วย

มีคุณลักษณะเฉพาะ ดังนี้

- มีหน่วยประมวลผลกลาง (CPU) แบบ ๒๔ แกนหลัก (๒๔ core) หรือดีกว่า สำหรับคอมพิวเตอร์แม่ข่าย (Server) โดยเฉพาะและมีความเร็วสัญญาณนาฬิกาพื้นฐาน ไม่น้อยกว่า ๒.๑๐ GHz จำนวนไม่น้อยกว่า ๒ หน่วย
- หน่วยประมวลผลกลาง (CPU) รองรับการประมวลผลแบบ ๖๔ bit มีหน่วยความจำแบบ Cache Memory รวมในระดับ (Level) เดียวกันไม่น้อยกว่า ๑๖ MB
- มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า ขนาดไม่น้อยกว่า ๒๕๖ GB
- สนับสนุนการทำงาน RAID ไม่น้อยกว่า RAID ๐, ๑, ๕
- มีหน่วยจัดเก็บข้อมูลชนิด SSD หรือดีกว่า และมีความจุไม่น้อยกว่า ๑.๒ Tb จำนวนไม่น้อยกว่า ๘ หน่วย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐G Base-T จำนวนไม่น้อยกว่า ๔ ช่อง
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑G Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๒ ช่อง
- มี Power Supply แบบ Redundant หรือ Hot Swap จำนวน ๒ หน่วย
- มีซอฟต์แวร์สำหรับให้บริการเครื่องคอมพิวเตอร์แบบเสมือนโดยมีคุณลักษณะพื้นฐานดังนี้
  - สามารถเรียกงานระบบงาน ผ่าน Web Browser หรือ GUI ได้
  - สามารถจัดสรรแบ่งส่วนทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย เช่น หน่วยประมวลผลกลาง (CPU), หน่วยความจำ (Memory) และหน่วยจัดเก็บข้อมูล (Storage) ให้เป็นเครื่องแม่ข่ายเสมือนสำหรับใช้งานได้
  - มีเครื่องมือบริหารการจัดส่วนกลางสำหรับช่วยสร้าง แก้ไข สำเนา หรือ ลบเครื่องคอมพิวเตอร์เสมือนได้
  - รองรับการสร้างคอมพิวเตอร์เสมือนแบบ Linux Container-based Virtualization
  - รองรับการกำหนด Firewall Policy ได้ทั้งระดับคลัสเตอร์คอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์เสมือน
  - สามารถทำ VM Live Migration ระหว่าง Node โดยไม่มี Downtime
  - มีเครื่องมือบริหารจัดการส่วนกลาง (Centralize Management) และมีสิทธิ์ที่สามารถใช้สร้างและบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่ายเสมือนได้เพียงพอต่อการใช้งาน

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- สามารถสร้าง ลบ แก้ไข กลุ่มเน็ตเวิร์คจากเครื่องมือบริหารจัดการส่วนกลางในการกำหนดค่าเพียงครั้งเดียวเพื่อให้ง่ายต่อการจัดการได้
- รองรับการใช้งานคอมพิวเตอร์แม่ข่ายเสมือนที่ใช้ระบบปฏิบัติการอย่างน้อยดังนี้ Windows Server, Redhat, SUSE, CentOS และ Ubuntu
- สามารถย้ายเครื่องคอมพิวเตอร์แม่ข่ายเสมือนจากเครื่องคอมพิวเตอร์แม่ข่ายเครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งโดยไม่ทำให้บริการบนเครื่องแม่ข่ายเสมือนหยุดทำงาน
- สามารถกำหนดค่า IP Address แบบ DHCP ให้กับเครื่องคอมพิวเตอร์เสมือนในแต่ละกลุ่มเน็ตเวิร์ค ภายในระบบ Virtualization ที่สร้างขึ้นได้
- สามารถตรวจสอบสถานะและการใช้งานทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่อง เช่น Name, CPU, Memory, Storage, IP address ได้
- สามารถตรวจสอบ IO Bandwidth หรือ IOPS หรือ Disk IO หรือ Latency รวมของเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมด (Cluster), ของแต่ละเครื่องคอมพิวเตอร์แม่ข่าย และของแต่ละเครื่องคอมพิวเตอร์เสมือนได้
- สามารถตรวจสอบประสิทธิภาพและแสดงสถานะประสิทธิภาพ (Health-Check) ของหน่วยประมวลผลกลาง (CPU) หน่วยความจำหลัก (Memory) ของเครื่องคอมพิวเตอร์เสมือน และ ของเครื่องคอมพิวเตอร์แม่ข่ายและ Cluster ได้

๕.๑.๑.๒ อุปกรณ์ควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (NAC: Network Access Control) จำนวน ๒ เครื่อง

มีคุณลักษณะเฉพาะ ดังนี้

- ระบบที่เสนอต้องเป็นอุปกรณ์ที่ออกแบบมาเพื่อทำหน้าที่ Network Access Control (NAC) โดยเฉพาะ
- มีความสามารถในการมองเห็น หรือตรวจพบอุปกรณ์ และผู้ใช้งานในเครือข่าย รวมถึงแสดงรายละเอียดอุปกรณ์แบบ headless device ในลักษณะโปรไฟล์ได้
- อุปกรณ์ที่เสนอมีคุณสมบัติ ดังนี้
  - O มี Storage ขนาด ๙๐๐GB แบบ SSD จำนวนไม่น้อยกว่า ๒ หน่วย
  - O มี Interface ๑GbE RJ๔๕ จำนวนไม่น้อยกว่า ๔ ports
  - O มี Power Supply แบบ Redundant พร้อมคุณสมบัติ Hot-Plug
  - O ผ่านการรับรองมาตรฐาน FCC, CE, ICES และ ROHS
  - O รองรับการกำหนดนโยบาย (Policy) และเปลี่ยนการตั้งค่า (Configuration) บนอุปกรณ์อย่างน้อยดังนี้
    - Network Infrastructure: Adtran, Aerohive, AlaxalA Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC,Apple,APRESIASystems, Avaya,Brocade/Foundry Networks/Ruckus,Cisco/Meraki,DLink,Extreme/ Enterasys/Siemens, H๓C, HP/Colubris/๓Com/Aruba,Intel, Juniper, NEC, Riverbed/Xirrus, and SonicWall
    - Security Infrastructure: Checkpoint, Cisco/Sourcefire, Cyphort, FireEye, Juniper/ Netscreen, Qualys, Sonicwall, Tenable

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- Authentication and Directory Services:
  - RADIUS: Cisco ACS, Free RADIUS, Microsoft IAS,
  - LDAP: Google SSO, Microsoft Active Directory, OpenLDAP
- Operation Systems: Android, Apple MAC OS X and iOS, Linux, Microsoft Windows

- สามารถตรวจสอบ (Scan) ระบบเครือข่าย เพื่อตรวจจับ และจัดสรรอุปกรณ์ได้ทั้งแบบ Agent และ Agentless และสร้างรายการอุปกรณ์ (Inventory) ที่ตรวจพบบนเครือข่ายได้
- เป็นอุปกรณ์ที่มีสถาปัยกรรมแบบ Centralized Architecture สามารถติดตั้งและบริหารจัดการได้จากส่วนกลาง (Centralized Deployment and Management)
- มีความสามารถทำ onboard แบบอัตโนมัติให้กับ Endpoint, User และ Guest ได้
- มีเทคนิคในการทำโพรไฟล์เพื่อตรวจสอบ User, Application และ Device บนเครือข่ายได้ไม่น้อยกว่า ๑๗ เทคนิค เช่น Active, Network Traffic, ONVIF, Passive, WinRM, WMI Profile, Script, IP Range, Location, Vendor OUI, SNMP, Persistent Agent, DHCP Fingerprinting, SNMP, TCP, UDP ได้เป็นอย่างน้อย
- สามารถกำหนด isolate และจำกัดการเข้าถึง VLAN กับอุปกรณ์ที่ตรวจพบการตั้งค่าไม่ตรงกับ Compliant หรือข้อกำหนดองค์กรได้
- สามารถทำงานได้แบบ out-of-band โดยไม่ต้องติดตั้งในระบบแบบ In-line และ Mirror เพื่อตรวจสอบทราฟฟิก
- สามารถกำหนด Policy ตามเงื่อนไข Location, User or host group และตามช่วงเวลา (Schedule) ได้
- สามารถกำหนด Portal สำหรับการเชื่อมต่อเครือข่าย และลงทะเบียนได้ โดยสามารถแยกตาม User/Host Profile ได้
- สามารถทำ Policy simulator โดยการจำลอง Host, Adapter และ User เพื่อทดสอบ Policy ก่อนใช้งานจริงได้
- สามารถกำหนดการแจ้งเตือน ตามเหตุการณ์ดังต่อไปนี้ได้ เป็นอย่างน้อย
  - Access Configuration Modified
  - Add/Modify/Remove Blocking via REST API
  - Certificate Expiration Warning in ๓๐ days and ๗ days
  - Maximum Concurrent Connections Critical and Exceeded
- อุปกรณ์ที่เสนอต้องมีแหล่งจ่ายไฟ (Power Supply) แบบ Hot Plug Redundant หรือ Hot-Swap Redundant

๕.๑.๑.๓ อุปกรณ์รักษาความปลอดภัยของระบบการสื่อสาร E-mail (E-mail Security Gateway) จำนวน ๒ เครื่อง

มีคุณลักษณะเฉพาะ ดังนี้

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

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T (RJ-๔๕) จำนวนไม่น้อยกว่า ๔ ช่อง
- มีพื้นที่เก็บข้อมูล (Storage) ขนาดไม่น้อยกว่า ๙๐๐GB จำนวนไม่น้อยกว่า ๒ หน่วย และรองรับการทำ Hardware RAID หรือ Software RAID ๐, ๑, ได้เป็นอย่างน้อย
- สามารถตรวจจับและป้องกันภัยคุกคามทางอีเมล์ ได้ทั้งขาเข้าและขาออก (Inbound & Outbound)
- อุปกรณ์ที่เสนอมีคุณสมบัติด้านความปลอดภัย ดังต่อไปนี้
  - สามารถตรวจสอบโดเมนผู้ส่งอีเมล์ตามมาตรฐาน SPF, DKIM และ DMARC ได้
  - ป้องกัน Spam จากเทคนิค Sender/Domain Reputation, Outbreak Protection, Heuristic/Behavior Analysis, Header Inspection, SURBBL/RBL และ Newsletter/Greymail Detection ได้
  - ตรวจสอบและป้องกัน URL ที่แนบมาตามประเภทของเว็บไซต์ ได้แก่ Spam, Malware/Malicious, Phishing, Pornography และ Newly Registered Domain ได้ หรือเทียบเท่า
  - มีคุณสมบัติป้องกัน Malware ได้
  - Cloud-Based Sandboxing
  - Content Disarm เพื่อจัดการ เช่น Remove ส่วน Active content หรือ Macro หรือ URL Hyperlink
  - ป้องกันการปลอมแปลงอีเมล์ (Business Email Compromise)
  - ตรวจสอบและป้องกัน URL ที่เป็นอันตรายภายในอีเมล์ (URL Click Protection)
  - สามารถควบคุมและป้องกันข้อมูลสูญหาย (Data Loss Prevention) ตามรูปแบบมาตรฐาน และสามารถกำหนดรูปแบบเองผ่าน RegEx (Regular Expression) ได้เป็นอย่างน้อย
  - สามารถทำ Email Encryption ได้
  - สามารถอัพเดตฐานข้อมูลด้านความปลอดภัยกับเจ้าของผลิตภัณฑ์ได้ตลอดระยะเวลารับประกัน
- สามารถเข้าบริหารจัดการตัวอุปกรณ์ผ่าน HTTPS หรือ SSH หรือดีกว่า
- สามารถเก็บ Log บนตัวเอง (Local Storage) ได้ พร้อมเสนอระบบออกรายงานส่วนกลางภายใต้เครื่องหมายการค้าเดียวกัน เพื่อรองรับการเก็บ Log และออกรายงานในระยะยาวได้
- สามารถแสดงรายงานรูปแบบของ HTML และ PDF ได้เป็นอย่างน้อย หรือเสนอระบบเพิ่มเติมได้
- รองรับทำงานในลักษณะ High Availability (HA) แบบ Active-Passive และ Active-Active ได้
- สามารถใช้งานตามมาตรฐาน IPv๖ ได้
- ผ่านการทดสอบและได้รับรองมาตรฐานที่เกี่ยวกับความปลอดภัยทางด้านอีเมล จาก VBSpam, NSS Labs, ICSA Labs และ SE Labs เป็นอย่างน้อย

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

๕.๑.๑.๔ ระบบจัดเก็บข้อมูลและระบบวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร (SIEM) จำนวน ๑ ระบบ
มีคุณลักษณะเฉพาะ ดังนี้

- เป็นระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ (Security Information and Event Management: SIEM) ประเภท Hardware Appliance โดยเฉพาะ ซึ่งประกอบด้วย
  - อุปกรณ์รวบรวมเหตุการณ์ (Collector) สำหรับระบบจัดเก็บข้อมูล จำนวน ๒ หน่วย แต่ละหน่วยมีคุณสมบัติ ดังนี้
    - ทำหน้าที่ค้นหาเครื่องคอมพิวเตอร์แม่ข่าย (Server) และ Monitor Performance พร้อม เก็บรวบรวม Log
    - ประมวลผลข้อมูลโดยการทำ Parsing และ Normalization ก่อนส่งให้กับ SIEM (pre-processing) ได้
    - ทำหน้าที่ Log Caching เหตุการณ์ หรือข้อมูล กรณีไม่สามารถติดต่อกับ SIEM ได้
    - มีหน่วยเก็บข้อมูล Storage ขนาด ๙๐๐GB ไม่น้อยกว่า ๔ หน่วย และหน่วยความจำ memory ไม่น้อยกว่า ๑๖ GB
    - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑G (RJ๔๕) จำนวนไม่น้อยกว่า ๔ พอร์ต
    - ระบบที่เสนอต้องประกอบด้วยอุปกรณ์รวบรวมเหตุการณ์ (Collector) จำนวนอย่างน้อย ๑ หน่วย
  - อุปกรณ์ SIEM สำหรับระบบวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ จำนวน ๑ หน่วยแต่ละหน่วยมีคุณสมบัติ ดังนี้
    - มีหน่วยเก็บข้อมูล Storage แบบ SSD หรือ NVMe ขนาดพร้อมใช้งาน (Useable) ขนาดรวมไม่น้อยกว่า ๑๐ TB และมีหน่วยเก็บข้อมูล HDD Storage ขนาดรวมไม่น้อยกว่า ๖๒TB พร้อมคุณสมบัติ Hot-Swappable
    - มีหน่วยความจำ Memory ไม่น้อยกว่า ๑๒๘ GB
    - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑G (RJ๔๕) จำนวนไม่น้อยกว่า ๒ พอร์ต และช่องแบบ ๒๕GE SFP๒๘ ไม่น้อยกว่า ๒ ช่อง และช่องแบบ ๑๐GE SFP+ ไม่น้อยกว่า ๒ ช่อง
    - สามารถรับ Log จาก Log Source ในรูปแบบ Syslog (TCP, UDP), WMI, NetFlow ได้เป็นอย่างน้อย
    - สามารถรับและวิเคราะห์ Log ได้ไม่น้อยกว่า ๒๐,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second)
    - สามารถเชื่อมโยงเหตุการณ์จาก Source ต่าง ๆ เข้าด้วยกัน (Correlation Rule) ทั้งแบบ Real-time หรือNearest Real-Time เพื่อหาต้นตอของภัยคุกคาม และสามารถ Customize เพิ่มเติมได้
    - มี Predefined Dashboard มาพร้อมกับระบบ เพื่อใช้สำหรับวิเคราะห์ข้อมูลเหตุการณ์ในรูปแบบของแผนภูมิ และตาราง และสามารถ Customize เพิ่มเติมได้

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- สามารถพิสูจน์ตัวตนผู้ใช้งานได้ โดยรองรับฐานข้อมูลผู้ใช้แบบ Local, Radius, LDAP และ SAML ได้เป็นอย่างน้อย
- สามารถเลือกบันทึกข้อมูลหรือเหตุการณ์ได้ทั้งใน Local Storage และ External Storage
- สามารถวิเคราะห์เปรียบเทียบข้อมูลระหว่างไอพีแอดเดรสกับรายชื่อผู้ใช้งานที่ใช้งาน IP Address นั้น ๆ อยู่ (Identity Mapping)
- มี Predefined Report ไม่น้อยกว่า ๑๐ รูปแบบ และสามารถ Customize เพิ่มเติมได้
- สามารถแจ้งเตือนแบบ Real-Time หรือ Nearest Real-Time เมื่อมีเหตุการณ์ตรงตามเงื่อนไข ที่สร้างไว้ และเหตุการณ์ผิดปกติของตัวอุปกรณ์ ผ่าน Email และ SNMP ได้เป็นอย่างน้อย
- สามารถเรียกใช้สคริปต์อัตโนมัติ เพื่อลดหรือจำกัดภัยคุกคาม (Automated Incident Mitigation) โดยมีสคริปต์มาพร้อมใช้ได้
- สามารถบริหารจัดการผ่านช่องทางที่มีการเข้ารหัสเช่น HTTPs และ SSH ได้เป็นอย่างน้อย
- สามารถจัดทำรายงานที่เกี่ยวข้องกับมาตรฐาน PCI, NIST, SANS ได้เป็นอย่างน้อย
- สามารถแสดงผลของเหตุการณ์ที่ถูกตรวจจับ โดยแยกตามหมวดหมู่ของ MITRE ATT&CK โดยรองรับทั้ง IT View และ ICS View
- สามารถตรวจสอบการเปลี่ยนแปลงค่า Configuration แบบ Real-Time หรือ Nearest Real-Time ของอุปกรณ์ Network ได้เป็นอย่างน้อย
- สามารถตรวจจับการเปลี่ยนแปลง Files, Folder, Windows Registry ได้
- รองรับการตรวจสอบพฤติกรรมของผู้ใช้ในระบบได้ (UEBA) ได้ในอนาคต
- สามารถปิดบังข้อมูลบางส่วน เช่น User, Email, IP Address ด้วยวิธี Data Masking หรือ Data Obfuscation เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลได้
- สามารถอัพเดทฐานข้อมูลด้านความปลอดภัย (IOC) แบบอัตโนมัติได้จากเจ้าของผลิตภัณฑ์ ตามระยะเวลาการรับประกัน
- ผลิตภัณฑ์ที่เสนอ มีเครื่องหมายการค้า หรือระบบปฏิบัติการที่มีผลการทดสอบ หรือได้รับการยอมรับดังต่อไปนี้
  - อยู่ในกลุ่ม Leader ด้าน Intelligent SIEM Platform จาก Kuppinger Cole ประจำปี ๒๐๒๒ หรือปีล่าสุด
  - อยู่ในกลุ่ม Challenger หรือ Leader ด้าน SIEM จาก Gartner Magic Quadrant ประจำปี ๒๐๒๓ หรือปีล่าสุด

๕.๑.๑.๕ ระบบตรวจจับภัยคุกคามและตอบสนองต่อระบบเครือข่ายคอมพิวเตอร์ (Network Detection and Response: NDR) จำนวน ๒ ระบบ
มีคุณลักษณะเฉพาะ ดังนี้

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- เป็นอุปกรณ์แบบ appliance ที่ออกแบบมาทำหน้าที่เป็นนักวิเคราะห์ความปลอดภัยเสมือน (Virtual Security Analyst) เพื่อระบุ จัดประเภท และตอบสนองต่อภัยคุกคามที่พรางตัวได้ดีโดยใช้ Artificial Intelligence (AI) และมีคุณสมบัติตรวจสอบความผิดปกติบนเครือข่าย (Network Anomaly) ได้
- เป็นอุปกรณ์ที่มีลักษณะการทำงานแบบ On-Premise และสามารถรองรับข้อมูล (Traffic Input) ได้แก่ Sniffer, ICAP, HTTPS API Upload, SMB/NFS, OFTP และ HTTP๒ ได้
- มีช่องเชื่อมต่อ ๑GE แบบ RJ๔๕ ไม่น้อยกว่า ๒ พอร์ต และแบบ ๑๐GE SFP+ ไม่น้อยกว่า ๔ ช่อง
- มี Power Supply แบบ redundant พร้อมคุณสมบัติ Hot Swappable
- มีคุณสมบัติในการตรวจสอบข้อมูลทางเครือข่าย ได้ดังต่อไปนี้
  - รองรับโปรโตคอล TCP, UDP, ICMP, ICMP๖, TLS, HTTP, SMB, SMTP, SSH, FTP, POP๓, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL และ PGSQL ได้เป็นอย่างน้อย
  - แสดงผล Device Inventory บนเครือข่าย โดยแสดงข้อมูล IP, Status (Online/Offline), Category (Phone, Computer, Firewall), Model, Vendor, Country ได้เป็นอย่างน้อย
  - แสดงผล Botnet บนเครือข่าย โดยแสดงข้อมูล Botnet Name, Severity, Timestamp (First and Latest), Count ได้เป็นอย่างน้อย
  - แสดงผล URL และ IP ที่มีความเสี่ยงได้ โดยแสดงข้อมูล URL Category, Severity, IOC หรือ Path ที่มีความเสี่ยง, Timestamp ได้เป็นอย่างน้อย
  - รองรับการแสดงผล Network Attack ที่ได้จากฐานข้อมูล IPS ของระบบเพื่อตรวจจับความผิดปกติบนเครือข่ายได้ทั้ง North-South และ East-West ตามข้อมูล Sniffer ที่ได้รับ
  - แสดงผลข้อมูล Weak/Vulnerable Communication บนเครือข่ายได้ เช่น Weak TLS version and cipher, SMB Protocol (Outdate Version, Level Security), Risky Flag on SNMP, Weak Encryption Option, Weak Server Version ได้เป็นอย่างน้อย
  - สามารถตรวจสอบ Encrypted Attack โดยใช้ JA๓ hash และ Server SSL Fingerprint ได้เป็นอย่างน้อย
  - สามารถตรวจสอบข้อมูลบนเครือข่ายโดยใช้ Machine Learning และสามารถเพิ่ม Feedback ผลการตรวจพบได้ เช่น Mark as Not Anomaly, Mark as Anomaly หรือเทียบเท่า ได้เองโดยผู้ดูแลระบบ
- มีคุณสมบัติการตรวจสอบในระดับไฟล์ได้ ดังต่อไปนี้
  - มีคุณสมบัติตรวจสอบ File Type โดยใช้ AI ได้แก่ ๓๒ bit and ๖๔ bit PE, PDF, MSOFFICE, HTML, ELF, VBS, VBA, JS, PHP, HWP Hangul_Office, XML, POWERSHELL, UPX, ASPACK, NSIS, AUTOIT, MSOFFICEX, RTF,

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, DOTNET, INNO, IFRAME ได้เป็นอย่างน้อย

- สามารถใช้ AI หรือ ANN ตรวจสอบมัลแวร์บน Remote File Location ผ่าน SMB และNFS ได้ พร้อมสามารถกำหนด Path เพื่อย้าย Quarantine File แยกจากส่วนเดิมได้
- สามารถรับการ Upload ไฟล์โดยตรงผ่าน GUI และ API
- สามารถทำงานร่วมกับ NGFW แบบ Inline Blocking โดย NGFW ควบคุม User Session ไว้ จนกว่าการตรวจสอบโดยระบบ NDR ที่เสนอตรวจสอบไฟล์จะแล้วเสร็จ
- รองรับการทำงานร่วมกับ NGFW, Mail Security, Sandbox, WAAP, Secure Web Gateway (Proxy), SOAR ได้เป็นอย่างน้อย

- มีคุณสมบัติแสดงข้อมูลที่ตรวจพบตาม Mitre Attack Tactics ได้ ทั้งในระดับ Network Session และ File
- มี AI ที่ประกอบด้วยคุณลักษณะมัลแวร์ไม่น้อยกว่า ๖ ล้านรายการ เพื่อใช้สนับสนุนการตัดสินมัลแวร์ได้ทันทีที่ติดตั้ง พร้อมความสามารถในการเรียนรู้คุณลักษณะใหม่ได้
- สามารถใช้ AI จำแนกมัลแวร์ หรือการโจมตีออกเป็นตามประเภท หรือสถานการณ์ได้ เช่น Worm Activity, Wiper, Fileless, Industroyer, Ransomware, Botnet, Exploit, Rootkit, Backdoor, Data Leak, Banking Trojan, Phishing, Search Engine Poisoning, Cryptojacking, Web Shell เป็นอย่างน้อย เพื่อใช้ข้อมูลดังกล่าวสนับสนุนการทำงานนักวิเคราะห์ความปลอดภัย
- รองรับการทำงานร่วมกับ Active Directory (AD) หรือ DNS เพื่อรับข้อมูล Hostname ของ Device ในเครือข่าย
- สนับสนุน Malware Analysis Throughput ไม่น้อยกว่า ๑๗๐,๐๐๐ ไฟล์ต่อชั่วโมง
- รองรับ sniffer throughput ไม่น้อยกว่า ๑๐G
- อุปกรณ์ที่เสนอต้องผ่านมาตรฐาน FCC Part ๑๕ Class A, VCCI, CE, UL และ CB

๕.๑.๑.๖ อุปกรณ์วิเคราะห์ข้อมูลระบบเครือข่ายและออกรายงานแบบรวมศูนย์

จำนวน ๑ เครื่อง

มีคุณลักษณะเฉพาะ ดังนี้

- เป็นอุปกรณ์ Hardware Appliance ที่สามารถเก็บรวบรวมเหตุการณ์ (Logs or Events) และรองรับการออกรายงานได้
- สามารถจัดเก็บข้อมูล Log เพื่อวิเคราะห์ (Analytic Rate) ได้ไม่น้อยกว่า ๔๐,๐๐๐ Logs/Events per second
- รองรับ Log เพื่อจัดเก็บ (Collector) ได้ไม่น้อยกว่า ๖๐,๐๐๐ Logs/events per Second
- สามารถจัดเก็บ Log ได้ในปริมาณไม่น้อยกว่า ๓,๐๐๐ GB ต่อวัน

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑ GE จำนวนไม่น้อยกว่า ๒ พอร์ต และช่องเชื่อมต่อระบบเครือข่ายแบบ ๒๕ GE SFP๒๘ จำนวนไม่น้อยกว่า ๒ พอร์ต
- มี Storage แบบ Hot Swappable ความจุพร้อมใช้งาน (Usable Storage After RAID) ไม่น้อยกว่า ๕๐ TB และรองรับการทำ RAID ๐/๑/๕/๖/๑๐/๕๐/๖๐ ได้เป็นอย่างน้อย
- มีแหล่งจ่ายไฟแบบ Redundant Hot Swappable จำนวนไม่น้อยกว่า ๒ หน่วย
- สามารถตรวจสอบความถูกต้องของข้อมูลที่จัดเก็บ (Checksum) ตามมาตรฐาน MD๕ หรือ SHA-๑ หรือดีกว่า
- สามารถแสดงสถานะและข้อมูลของระบบที่ส่ง log เข้ามา ได้ดังต่อไปนี้ Average Log Rate (Log/Sec), พื้นที่ Storage ที่ใช้เพื่อจัดเก็บข้อมูลของระบบดังกล่าว (Device Storage), Firmware Version, Serial Number, IP Address
- สามารถบริหารจัดการอุปกรณ์ผ่านโปรโตคอล HTTPS ผ่าน Web Browser ได้โดยตรง โดยไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติม และโปรโตคอล SSH ได้เป็นอย่างน้อย
- สามารถแสดงข้อมูลในรูปแบบ Dashboard ได้อย่างน้อยดังต่อไปนี้
  - แสดงข้อมูล Top Threats ที่ประกอบด้วย CVE ID, Threat Level (Critical, High, Medium, Low), จำนวนครั้งที่เกิดขึ้น (Incidents) พร้อมแสดงข้อมูลเปรียบเทียบ ในลักษณะกราฟเส้นและกราฟแท่ง ได้เป็นอย่างน้อย
  - แสดงข้อมูลการใช้งาน ได้แก่ Top Source, Top Destinations, Top Country/Region, Policy Hit, Top Application, Top Website Domain, Top Website Categories โดยเลือกแสดงผลในลักษณะกราฟเส้นและกราฟแท่งได้เป็นอย่างน้อย
- สามารถกำหนดช่วงเวลาของข้อมูลที่ต้องการแสดงผลแบบราย ๕ นาที, รายชั่วโมง, รายวัน, รายสัปดาห์ และกำหนดช่วงเวลาเพิ่มเติม (Custom) ได้เป็นอย่างน้อย
- สามารถแสดงข้อมูล Resource Usage ได้ดังต่อไปนี้ CPU Usage, Memory Usage, Concurrent Session, New Sessions โดยแสดงได้
- ทั้งแบบค่าเฉลี่ย (Average) และค่าสูงสุด (Peak)
- มีคุณสมบัติในการออกรายงานได้อย่างน้อยดังต่อไปนี้
  - มีรูปแบบรายงานไม่น้อยกว่า ๕๐ รูปแบบ เช่น ๓๖๐ Protection Report, Admin and System Events Report, Cyber Threat Assessment, PCI-DSS Compliance, Data Loss Prevention Detailed Report ได้เป็นอย่างน้อย
  - สามารถแสดงข้อมูล Log เช่น Date, Time, Source IP, User, Destination IP และ Services ได้เป็นอย่างน้อย

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- สามารถปรับแต่งรายงาน (Customize) และ คัดลอกรูปแบบรายงาน (Clone) จากรายงานเดิมได้
- สามารถตั้งเวลาการออกรายงาน (Schedule Report) ได้
- สามารถแสดงรายงานในรูปแบบของ PDF, HTML และ CSV ได้เป็นอย่างน้อย

- สามารถส่งต่อข้อมูล log ไปยังระบบอื่นได้ ในรูปแบบ SYSLOG และ CEF Format ได้
- ได้รับการรับรองตามมาตรฐาน FCC Part ๑๕ Class A, RCM, VCCI, CE, UL/ cUL, CB เป็นอย่างน้อย

๕.๑.๑.๗ อุปกรณ์กระจายสัญญาณ (L๓ Switch) ๑๐Gbps ขนาด ๒๔ ช่อง
จำนวน ๔ เครื่อง

มีคุณลักษณะเฉพาะ ดังนี้

- มีลักษณะการทำงานไม่น้อยกว่า Layer ๓ ของ OSI Model
- สามารถค้นหาเส้นทางเครือข่ายโดยใช้โปรโตคอล (Routing Protocol) RIP,BGP และ OSPF ได้เป็นอย่างน้อย
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐GE Base-T หรือ SFP+ จำนวนไม่น้อยกว่า ๒๔ ช่อง
- มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ QSFP+ หรือ QSFP๒๘ จำนวนไม่น้อยกว่า ๒ ช่อง
- มีสัญญาณไฟแสดงสถานะของการทำงานช่องเชื่อมต่อระบบเครือข่ายทุกช่อง
- มี Switching Capacity ไม่น้อยกว่า ๘๐๐ Gbps
- รองรับ Mac Address ได้ไม่น้อยกว่า ๖๔K Mac Address และรองรับ VLANs ไม่น้อยกว่า ๒K
- สามารถใช้งานตามมาตรฐาน IPv๖ ได้
- สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ Command Line Interface (CLI) ได้
- สามารถส่งข้อมูล Log File ในรูปแบบ Syslog ได้เป็นอย่างน้อย
- มี Power Supply แบบ Redundancy หรือ Hot Swap หรือ Dual Hot Swappable จำนวน ๒ หน่วย

๕.๑.๑.๘ ตู้สำหรับจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ แบบที่ ๒ (ขนาด ๔๒U)
จำนวน ๒ หน่วย

มีคุณลักษณะเฉพาะ ดังนี้

- เป็นตู้ Rack ปิด ขนาด ๑๙ นิ้ว ๔๒U โดยมีความกว้างไม่น้อยกว่า ๖๐ เซนติเมตร ความลึกไม่น้อยกว่า ๑๑๐ เซนติเมตรและความสูงไม่น้อยกว่า ๒๐๐ เซนติเมตร
- ผลิตจากเหล็กแผ่นเคลือบสังกะสีแบบชุบด้วยไฟฟ้า (Electro-galvanized steel sheet)
- มีช่องเสียบไฟฟ้า จำนวนไม่น้อยกว่า ๑๒ ช่อง
- มีพัดลมสำหรับระบายความร้อน ไม่น้อยกว่า ๒ ตัว

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

๕.๑.๒ ระบบคอมพิวเตอร์ซอฟต์แวร์

๕.๑.๒.๑ ซอฟต์แวร์ระบบป้องกันและควบคุมการใช้งานของเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint Protection) จำนวน ๕๐๐ หน่วย

มีคุณลักษณะเฉพาะ ดังนี้

- เป็นซอฟท์แวร์สำหรับติดตั้งบนเครื่องผู้ใช้ปลายทางเพื่อช่วยเพิ่มความปลอดภัยบนเครื่องคอมพิวเตอร์สำหรับองค์กร (Endpoint Security)
- มีลิขสิทธิ์การใช้งานได้ไม่น้อยกว่า ๕๐๐ Licenses
- รองรับการพิสูจน์ตัวตน (Authentication) โดยทำงานร่วมกับ Local User, AD, LDAP และ SAML ได้เป็นอย่างน้อย
- สามารถทำ SSL และ IPSec VPN และมีคุณสมบัติ Auto-connect and Always-up เพื่อความสะดวกในการใช้งาน
- สามารถทำ Split Tunnel การใช้งาน VPN ได้ตามเงื่อนไข IP Address หรือ Application ได้เป็นอย่างน้อย
- มีคุณสมบัติด้านความปลอดภัย สำหรับเครื่องลูกข่ายที่ติดตั้งซอฟต์แวร์อย่างน้อยดังนี้
  - Anti-Virus หรือ Anti-Malware
  - Application Control
  - สามารถตรวจหาช่องโหว่ (Vulnerability Scan) บนเครื่องผู้ใช้งาน โดยแสดงผลช่องโหว่ที่ตรวจพบ พร้อมระดับความอันตรายได้ เช่น Critical, High, Medium, Low ได้เป็นอย่างน้อย หรือเทียบเท่า
  - ควบคุมการใช้งานเว็บทราฟฟิค ตามประเภทเว็บไซต์ได้ (URL Category) โดยใช้ฐานข้อมูลประเภทเว็บไซต์เดียวกันกับ NGFW ของสำนักบริหารการทะเบียน และสามารถรับอัพเดตได้ตลอดระยะเวลารับประกัน
  - สามารถตรวจสอบคุณสมบัติของเครื่องลูกข่าย (Security Posture) เช่น Certificate, Vulnerability Status, Anti-Virus Update Status, Operating Systems, File, Domain, Registry ได้เป็นอย่างน้อย
  - สามารถทำงานร่วมกับ NGFW ของสำนักบริหารการทะเบียน เพื่อกำหนด Policy การเข้าถึงเครือข่าย ตามคุณสมบัติของเครื่องลูกข่าย แบบ Zero-Trust เช่น IP, MAC, Users, Certificate, Vulnerability Status, Anti-Virus Update Status, Operating Systems ได้เป็นอย่างน้อย หรือเสนอระบบเพิ่มเติมภายใต้เครื่องหมายการค้าเดียวกัน เพื่อให้มีคุณสมบัติตามที่กำหนด
- มีระบบบริหารจัดการซอฟต์แวร์ที่ติดตั้งบนเครื่องผู้ใช้ได้จากส่วนกลาง (Centralized Management) ผ่าน web browser ได้โดยตรง
- รองรับการติดตั้ง Agent บนเครื่องคอมพิวเตอร์ลูกข่าย (Endpoint) ได้แก่ Microsoft Windows, Mac OS, iOS, Android, Ubuntu, CentOS และ Red hat ได้เป็นอย่างน้อย

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

๕.๑.๒.๒ ระบบป้องกันการเข้าถึงข้อมูลระดับสูง (Privileged Account Security Management) จำนวน ๑ ระบบ

มีคุณลักษณะเฉพาะ ดังนี้

- เป็นระบบที่ออกแบบมาโดยเฉพาะเพื่อทำหน้าที่ควบคุมความปลอดภัยในการใช้งาน Privileged Account โดยสามารถบริหารจัดการรหัสผ่านและควบคุมเฝ้าระวังการใช้งาน Privileged Session เพื่อลดความเสี่ยงจากการถูกโจมตีและสามารถตอบโจทย์ตามความต้องการของ Compliance ได้
- ผลิตภัณฑ์ที่นำเสนอจะต้องได้รับการรับรองอยู่ในกลุ่ม Leader ด้าน Privileged Access Management จากหน่วยงานที่ทำการวิจัยตลาดชั้นนำ (Gartner) ในปี ๒๐๒๓ เป็นอย่างน้อย
- สามารถตรวจสอบและวิเคราะห์ภัยคุกคามจากพฤติกรรมการใช้งาน (Privileged Threat Analytics) ได้
- สามารถเข้ารหัสข้อมูลของ Privileged Account ด้วย Algorithm แบบ AES-๒๕๖, RSA-๒๐๔๘ หรือดีกว่า โดยผ่านการรองรับมาตรฐาน FIPS ๑๔๐-๒
- ระบบที่นำเสนอต้องมี Multifactor Authentication หากไม่รองรับสามารถเสนออุปกรณ์หรือ customize เพิ่มเติมเพื่อให้สามารถทำงานได้โดยประสิทธิภาพของระบบไม่ลดลง
- รองรับรูปแบบการ Authentication แบบ Username/Password (Local database), RSA SecurID, Web SSO, RADIUS, PKI, และ LDAP ได้เป็นอย่างน้อย
- สามารถบริหารจัดการบัญชีผู้ใช้งานและรหัสผ่านของระบบต่อไปนี้ได้เป็นอย่างน้อย
  - Operating Systems Windows, Linux Redhat, VMWare ESX/ESXi
  - Windows Applications: Service accounts, Scheduled Tasks, IIS Application Pools
  - Databases Oracle, MSSQL, DB๒, Informix, Sybase, MySQL
  - รองรับ Network/Security Appliances ได้อย่างน้อยดังนี้ CheckPoint Firewall,Cisco,Fortinet,Palo Alto Networks

  หรือหากไม่รองรับสามารถเสนออุปกรณ์หรือ Customize เพิ่มเติมเพื่อให้สามารถทำงานได้โดยประสิทธิภาพของระบบไม่ลดลง
- สามารถตรวจหาบัญชีผู้ใช้งานบนระบบปลายทางผ่าน Active Directory และเพิ่มบัญชีผู้ใช้งานในระบบได้ (Automatic Discovery and Provisioning)
- สามารถบริหารจัดการรหัสผ่านตามคุณสมบัติดังนี้ได้เป็นอย่างน้อย
  - สามารถเปลี่ยนรหัสผ่านของ Privileged Account ตามช่วงเวลาที่กำหนดและหลังจากการใช้งานโดยอัตโนมัติ (One-time Password)
  - สามารถกำหนดความยาว และองค์ประกอบของรหัสผ่าน เช่น ตัวอักษรตัวใหญ่ (Upper Case), ตัวอักษรตัวเล็ก (Lower Case), ตัวเลข (Digit) และอักขระพิเศษ (Special Character)
  - สามารถเก็บประวัติการเปลี่ยนรหัสผ่าน (Password History)
  - สามารถกำหนด Workflow ในการใช้งานตามคุณสมบัติดังนี้ได้เป็นอย่างน้อย

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- สามารถทำงานแบบ Dual Control โดยผู้ใช้ต้องได้รับการอนุมัติก่อนที่จะใช้งานได้ และต้องสามารถกำหนดรูปแบบการทำงานดังต่อไปนี้ได้เป็นอย่างน้อย
  - กำหนดจำนวนผู้อนุมัติขั้นต่ำ
  - กำหนดลำดับขั้นในการอนุมัติ
  - แจ้งเตือนทางอีเมลในกระบวนการร้องขอและอนุมัติ
- สามารถป้องกันการเข้าถึงรหัสผ่านในช่วงระยะเวลาเดียวกันได้ (Check-in/ Check-out Exclusive Access)

- ต้องมี Web portal ที่ออกแบบเฉพาะสำหรับอุปกรณ์ mobile เพื่อใช้ในการร้องขอรหัสผ่าน และอนุมัติการใช้งานเพื่อความสะดวกในการใช้งานจากอุปกรณ์ เช่น Smart Phone หากไม่รองรับสามารถเสนออุปกรณ์หรือ Customize เพิ่มเติมเพื่อให้สามารถทำงานได้โดยประสิทธิภาพของระบบไม่ลดลง
- สามารถเปลี่ยนรหัสผ่านแบบ Hard-code ได้โดยอัตโนมัติ โดยต้องเปลี่ยนรหัสผ่านบน Configuration files, Windows Services, Windows Scheduled Tasks, และ Windows IIS Application Pools ได้เป็นอย่างน้อย หากไม่รองรับสามารถเสนออุปกรณ์หรือ Customize เพิ่มเติมเพื่อให้สามารถทำงานได้โดยประสิทธิภาพของระบบไม่ลดลง
- สามารถเชื่อมต่อไปยังระบบปลายทาง (Transparent Connection) ตามคุณสมบัติดังนี้ได้เป็นอย่างน้อย
  - สามารถเข้าสู่ระบบปลายทางโดยไม่ต้องแสดงรหัสผ่านให้ผู้ใช้ทราบ
  - สามารถเชื่อมต่อไปยังระบบปลายทางผ่าน application โดยใช้ Universal Connector ได้ โดยต้องรองรับ application ดังนี้ Microsoft SQL Management Studio, CheckPoint SmartDashboard, WinSCP, VMWare VSphere Client ได้เป็นอย่างน้อย
- สามารถบันทึกการใช้งาน Privileged Session ในรูปแบบของ Video Recordings, Keystrokes, และ Commands ดังต่อไปนี้ได้เป็นอย่างน้อย
  - Privileged SSH Sessions ในรูปแบบของ Commands List
  - Privileged SQL Commands ในรูปแบบของ SQL Commands
  - Privileged Windows Sessions ในรูปแบบของ Windows Process และ Windows Title
- สามารถค้นหาบันทึกการใช้งานจาก Commands, Keystrokes, และ Windows Events ได้แบบ Free Text Search
- สามารถทำ White-listing และ Black-listing สำหรับ SSH Commands เพื่อป้องกันการรันคำสั่งที่ไม่อนุญาตบนระบบที่ควบคุมได้ โดยไม่ต้องติดตั้ง Agent
- สามารถเฝ้าระวัง (Monitor) การใช้งาน Privileged Session ได้แบบ Real-time และสามารถตัดการเชื่อมต่อ (Terminate) ได้ทันทีโดยผู้ดูแลระบบเมื่อพบพฤติกรรมที่ผิดปกติ

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- สามารถตรวจสอบและวิเคราะห์ภัยคุกคามจากพฤติกรรมการใช้งาน (Privileged Threat Analytics) ได้ตามคุณสมบัติดังนี้ได้เป็นอย่างน้อย
  - สามารถกำหนดเงื่อนไขเพื่อตรวจสอบพฤติกรรมการใช้งานที่มีความเสี่ยงสูง (High Risk Activities) และแสดงผลเป็น Risk Score เพื่อระบุระดับความเสี่ยงของแต่ละ Privileged Session ได้
  - สามารถตรวจสอบและวิเคราะห์พฤติกรรมการใช้งานของ Privileged User เพื่อสร้างเป็น Baseline และแจ้งเตือนหากพบพฤติกรรมที่ผิดปกติ
  - สามารถตรวจจับพฤติกรรมการใช้งานที่ผิดปกติได้ โดยสามารถ Suspend session หรือ Terminate session การใช้งานนั้นได้โดยอัตโนมัติ

  หากไม่รองรับสามารถเสนออุปกรณ์หรือ customize เพิ่มเติมเพื่อให้สามารถใช้งานได้โดยประสิทธิภาพของระบบไม่ลดลง
- สามารถทำงานในลักษณะ High Availability หรือ Disaster Recovery ได้
- สามารถทำงานร่วมกับระบบดังต่อไปนี้ได้เป็นอย่างน้อย
  - Ticketing System
  - Security Information and Event Management (SIEM)
  - Hardware Security Module (HSM)
- มีเครื่องมือเฉพาะสำหรับการ Backup หรือสามารถทำงานร่วมกับ Backup tools ได้
- อุปกรณ์ที่ทำหน้าที่เก็บข้อมูลสำคัญ (Vault) ต้องได้รับมาตรฐาน Common Criteria Certified EAL ๒+ เป็นอย่างน้อย
- ต้องมีระบบที่ออกแบบมาสำหรับใช้ในการรีโมททั้งจากบุคคลภายใน (Internal User) และบุคคลภายนอก (remote vendor) โดยเฉพาะ เพื่อเข้าถึงระบบที่อยู่ภายในองค์กรซึ่งถูกบริหารจัดการโดยระบบบริหารจัดการรหัสผ่าน

  หากไม่รองรับสามารถเสนออุปกรณ์หรือ customize เพิ่มเติมเพื่อให้สามารถทำงานได้โดยประสิทธิภาพของระบบไม่ลดลง
- ระบบที่นำเสนอสำหรับการใช้งานรีโมทต้องเป็นรูปแบบ SaaS
- การใช้งานรีโมทต้องสามารถทำ multifactor authentication โดยใช้ Biometric ที่เป็นความสามารถของ Smart Phone ได้
- การ Authentication โดยใช้ Biometric บน Smart Phone ต้องรอบรับ iOS และ Android เป็นอย่างน้อย
- ระบบที่นำเสนอสำหรับการใช้งานรีโมทต้องไม่มีการใช้งาน VPN Agent และ Credential ในการเข้าใช้งาน
- ระบบที่นำเสนอสำหรับการใช้งานรีโมทต้องสามารถทำ just-in-time Provisioning ได้

๕.๑.๒.๓ ซอฟต์แวร์ระบบการป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention/Data Leak Prevention: DLP) จำนวน ๕๐๐ หน่วย
มีคุณลักษณะเฉพาะ ดังนี้

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- ระบบสามารถทำการวิเคราะห์ และป้องกันการรั่วไหลของข้อมูลผ่านช่องทางเครือข่าย (DLP Network) และเครื่อง Endpoint (DLP Endpoint) ได้ โดยมีลิขสิทธิ์การใช้งานไม่น้อยกว่า ๕๐๐ Licenses
- ระบบบริหารจัดการ (Management server) รองรับการใช้งานร่วมกับฐานข้อมูล Microsoft SQL server ได้
- สามารถบริหารจัดการ และควบคุมนโยบายการตรวจสอบ DLP ได้จากส่วนกลาง (Centralized Management) ทั้งอุปกรณ์ DLP Network, DLP Endpoint และ DLP Discover ได้ และรองรับการทำงานร่วมกับ CASB ได้ในอนาคต
- ระบบที่นำเสนอต้องมี Pre-defined Policy ไม่น้อยกว่า ๑,๕๐๐ Policies โดยมีข้อมูลต้นแบบ ที่สามารถตรวจสอบข้อมูลลักษณะดังต่อไปนี้ได้เป็นอย่างน้อย
  - ข้อมูลระบุตัวตน Personally Identifiable Information (PII)
  - General Data Protection Regulation (GDPR) และ Payment Card Industry (PCI)
  - ข้อมูลบัตรเครดิต: American Express, JCB, Master card, Visa และ Union Pay
  - Software Source Code: C++, Java, Perl, และ Python
  - Protect Health Information (PHI): Credit cards and Common Medical Condition, DNA Profile, ICD๙ Code and Name, ICD๑๐ Code and Name, Medical Form และ NDC Number
- สามารถตรวจจับผู้ใช้งานที่พยายามส่งข้อมูลออกนอกองค์กร ด้วยวิธีการกระจายข้อมูลออกเป็นข้อมูลย่อย ๆ และส่งออกผ่านช่องทางต่าง ๆ หลาย ๆ ครั้งได้ (Drip DLP)
- สามารถตรวจจับพฤติกรรมน่าสงสัยของผู้ใช้ (Suspicious User Activity) ดังต่อไปนี้ได้เป็นอย่างน้อย
  - การส่งข้อมูล เช่น Source Code (C or Python), Office File ในช่วงเวลาไม่เหมาะสม (Data Sent During Unusual Hours)
  - การส่ง Email ถึงคู่แข่ง (Email to Competitor) เช่น Encrypted Attachment, Contact Information
  - การเปิดเผยรหัสผ่าน (Password Dissemination)
  - การส่ง Mail ถึงผู้ส่งเอง (Suspected Mail to Self) เช่น Archive Files, Confidential in Header/Footer, Encryption Files of Known/Unknown
- สามารถตรวจสอบเนื้อหาในไฟล์ฟอร์แมตต่าง ๆ เช่น Plain Text, Microsoft Office Documents (DOCX, PPTX, XLSX) และ PDF ได้
- สามารถทำ Database Fingerprint ได้ โดยเชื่อมต่อผ่าน ODBC และสามารถเลือก Fingerprint เป็นบาง Field หรือกำหนดผ่าน SQL Query ได้
- สามารถทำ Content Classification ได้ด้วยวิธีดังต่อไปนี้
  - Key Phrases, Dictionaries และ Regular Expression
  - File Properties

- Machine Learning
- Fingerprinting Files, Directories, SharePoint และ Database

- ระบบที่เสนอต้องมีหน้าจอแสดงผล Incident Management ที่ประกอบด้วย Incident Detail ในลักษณะ What, Where, Who, How ได้ โดยสามารถดูรายละเอียดของข้อมูลที่รั่วไหลออกไปในลักษณะ forensic ได้
- สามารถแสดงรายงาน Incident ในลักษณะ Risk Score ได้ (Incident Risk Ranking) โดยสามารถแสดงตาม Highest Risk User ที่มีความเสี่ยงมากที่สุด ๒๐ Cases ได้
- สามารถสร้างนโยบาย โดยการใช้ Logic ระหว่างเงื่อนไข เพื่อทำนโยบายการตรวจสอบข้อมูลได้แม่นยำมากขึ้น โดยสามารถใช้ logic ได้แก่ AND, OR, NOT และวงเล็บได้
- สามารถบริหารจัดการ Incident Workflow ที่เกิดขึ้นได้ โดยสามารถปรับเปลี่ยน Incident Severity และ Incident Status ได้ และสามารถบริหารจัดการ Email Incident โดยกำหนดให้ผู้ที่ได้รับมอบหมายสามารถอนุมัติหรือรับทราบผ่านอีเมลได้
- สามารถป้องกันข้อมูลรั่วไหล หากมีการส่งไฟล์รูปภาพที่มีข้อความ Text ปรากฏในรูปภาพผ่านทาง Web post และ อีเมล โดยการแปลงข้อความที่ปรากฏเป็น Key Phrase เพื่อตรวจสอบร่วมกับ DLP Policy ที่กำหนดไว้ด้วยเทคโนโลยี Optical Characteristic Recognition (OCR) ได้
- สามารถเรียกดูรายละเอียดเหตุการณ์ที่เกิดขึ้น (Incident) ประกอบด้วย วัน/เวลา, Address ผู้ส่ง/ผู้รับ, ผู้ที่ทำการละเมิด, นโยบายที่ละเมิด, โปรโตคอลที่ใช้, ไฟล์ต้นฉบับที่ถูกส่งออก และสามารถแจ้งเตือน (Notification) ผ่านอีเมลไปยังผู้ที่เกี่ยวข้องในกรณีที่พนักงานละเมิดนโยบาย

๕.๑.๓ อื่น ๆ

๕.๑.๓.๑ ปรับปรุงห้องศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (BORA CIRT) ตามแผนผังในภาคผนวก ๑
มีคุณลักษณะเฉพาะ ดังนี้

- งานสถาปัตยกรรม
  - ดำเนินการรื้อถอนผนัง ประตู หน้าต่าง เคาท์เตอร์ ระบบไฟฟ้าแสงสว่าง
  - ดำเนินการซ่อมแซมพื้นเดิมที่เสียหาย
  - จัดทำพื้นยกระดับ สูง ๓๐ เซนติเมตร ขนาดพื้นที่ ๒๗ ตารางเมตร พร้อมติดตั้งพรม
  - ทาสีผนัง สีขาว รอบห้องพื้นที่ ๒๕๐ ตารางเมตร โดยเป็นสีน้ำอะคริลิคแท้ ๑๐๐% ชนิดด้านหรือกึ่งเงา สามารถเช็ดล้างทำความสะอาดได้ง่าย ปราศจากสารตะกั่วและสารปรอท ทนทานต่อเชื้อราและตะไคร่น้ำ
  - จัดทำผนังสำหรับติดตั้ง VIDEO Wall ขนาด ๕๕ นิ้ว จำนวน ๘ จอ โดยออกแบบให้มีช่อง Service ให้สามารถใช้งานได้ง่าย

- ดำเนินการปรับปรุงฝ้า ให้เป็นแบบฉาบเรียบ โดยมีพื้นที่ ๑๐๐ ตารางเมตร พร้อมทาสีขาว และจัดทำช่อง Service
- จัดทำบิ้วท์อินเคาท์เตอร์รูปครึ่งวงกลม โดยให้มีขนาดรองรับเจ้าหน้าที่นั่งได้ ๔ คนเป็นอย่างน้อย
- จัดทำฉากกั้นโต๊ะทำงาน ที่มีความสูงไม่น้อยกว่า ๑๕๐ เซนติเมตร
- ติดตั้งประตูบานสวิงระหว่างห้องประชุม ขนาดไม่น้อยกว่า กว้าง ๑๑๐ x สูง ๓๒๐ เซนติเมตร
- ติดตั้งผนังกระจก Switchable Film ด้านหน้า ขนาดไม่น้อยกว่า กว้าง ๔๘๐ x สูง ๒๔๐ เซนติเมตร
- ติดตั้งผนังกระจก Switchable Film ห้องประชุม ขนาดไม่น้อยกว่า กว้าง ๑๙๐ x ๑๙๐ เซนติเมตร ทั้งหมด ๓ บาน
- จัดทำโลโก้ตัวอักษรสีทอง โดยกำหนดข้อความดังนี้ "ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (BORA CIRT) สำนักบริหารการทะเบียน กรมการปกครอง"
- จัดหาโต๊ะทำงานพร้อมเก้าอี้ทำงาน จำนวน ๒ ชุด
  มีคุณลักษณะดังนี้
  - โต๊ะทำงาน
    - โต๊ะทำงานต้องมีขนาดไม่น้อยกว่า ลึก ๗๕ x กว้าง ๑๕๐ x สูง ๗๕ เซนติเมตร
    - ต้องมีตู้ลิ้นชักหรือตู้เก็บของ ขนาดไม่น้อยกว่า ลึก ๔๐ x กว้าง ๘๐ x สูง ๖๐ เซนติเมตร
    - ปิดผิวด้วยวัสดุเมลามีน หรือเทียบเท่า หรือดีกว่า
  - เก้าอี้ทำงาน
    - เก้าอี้ต้องมีขนาดไม่น้อยกว่า ลึก ๕๕ x กว้าง ๕๕ x สูง ๘๕ เซนติเมตร
    - วัสดุหุ้มด้วยผ้า หรือผ้าตาข่าย
    - มีล้อเลื่อน
    - มีที่พักแขน
    - ต้องสามารถปรับระดับสูงต่ำได้
- จัดหาโต๊ะประชุม พร้อมเก้าอี้ มีที่นั่งประชุมได้ ๖ ที่ จำนวน ๑ ชุด
  มีคุณลักษณะดังนี้
  - โต๊ะประชุม
    - มีขนาดไม่น้อยกว่า ลึก ๑๐๐ x กว้าง ๑๘๐ x สูง ๗๕ เซนติเมตร
    - ปิดผิวด้วยวัสดุเมลามีนหรือลามิเนต หรือดีกว่า
    - ขาโต๊ะเป็นเหล็กหรืออลูมิเนียม หรือดีกว่า
  - เก้าอี้
    - มีขนาดไม่น้อยกว่า ลึก ๕๕ x กว้าง ๕๕ x สูง ๘๕ เซนติเมตร
    - วัสดุหุ้มด้วยผ้าหรือหนังเทียม หรือดีกว่า

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- มีล้อเลื่อน
- มีที่พักแขน
- สามารถปรับระดับสูงต่ำได้

- จัดหาชุดอุปกรณ์สำหรับระบบ Access Control จำนวน ๑ ชุด มีคุณลักษณะดังนี้
  - อุปกรณ์เครื่องควบคุมการเปิด-ปิดประตูด้วยใบหน้า
    - ตัวอุปกรณ์ต้องมีกล้องคู่ที่ความสามารถในการรับภาพมุมกว้าง (Wide Angle) รองรับการสแกนใบหน้า (Face Recognition)
    - มีคุณสมบัติการสแกนใบหน้า
    - มีคุณสมบัติการสแกนลายนิ้วมือ
    - รองรับการสแกนภาพใบหน้าได้ไม่น้อยกว่า ๑,๕๐๐ ภาพ
    - รองรับการสแกนลายนิ้วมือได้ไม่น้อยกว่า ๓,๐๐๐ รูป
    - รองรับการสแกนภาพใบหน้าที่ใส่หน้ากาก
    - รองรับการอ่านการ์ดบนความถี่ ๑๓.๕๖ MHz
    - มีหน้าจอแสดงผลแบบ LCD สัมผัสขนาดไม่น้อยกว่า ๔.๓ นิ้ว
    - รองรับการเชื่อมต่อผ่าน Local Area Network ความเร็วอย่างน้อย ๑๐/๑๐๐ Mbps
    - ตัวเครื่องสามารถรองรับการเชื่อมต่อผ่านพอร์ตสื่อสารแบบ RS-๔๘๕
    - ตัวเครื่องสามารถรองรับการเชื่อมต่อผ่านพอร์ตสื่อสารแบบ Wiegand
    - รองรับการเชื่อมต่อด้วยโปรโตคอล ISUP๕.๐, ISAPI
    - สามารถตั้งค่าต่าง ๆ ผ่าน Web Client ได้
    - ตัวเครื่องสามารถรองรับการรับส่งข้อมูลผ่านพอร์ตสื่อสารแบบ USB
    - อุปกรณ์สามารถทำงานภายใต้อุณภูมิตั้งแต่ -๓๐ ถึง ๖๐ องศาเซลเซียส
    - อุปกรณ์สามารถทำงานภายใต้ความชื้นสัมพัทธ์ตั้งแต่ ๐ ถึง ๙๐ เปอร์เซ็นต์
    - อุปกรณ์สามารถทำงานด้วยแรงดันไฟฟ้าแบบกระแสตรง ๑๒ โวลท์ ที่กระแสไฟฟ้า ๑ แอมแปร์ หรือดีกว่า
    - ตัวอุปกรณ์รองรับและสามารถปรับเปลี่ยนภาษาได้ทั้งภาษาไทยและภาษาอังกฤษ โดยมีให้เลือกอย่างน้อยไม่ต่ำกว่า ๒ ภาษา

- จัดหา VIDEO Wall ขนาด ๕๕ นิ้ว จำนวน ๘ จอ พร้อมขาแขวน มีคุณลักษณะดังนี้
  - อุปกรณ์ต้องมีขนาดจอไม่น้อยกว่า ๕๕ นิ้ว
  - หน้าจอแสดงผล LCD ความละเอียดไม่น้อยกว่า ๑๙๒๐ x ๑๐๘๐ pixels

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- มีค่าความสว่างไม่น้อยกว่า ๕๐๐ cd/m²
- มีมุมมองในแนวราบและแนวตั้งไม่น้อยกว่า ๑๕๐ องศา
- ต้องมีอัตราความชัด (Contrast) ไม่น้อยกว่า ๑๒๐๐:๑
- สามารถทำงานได้ในอุณหภูมิ ๐ องศา ถึง ๔๐ องศา หรือดีกว่า
- สามารถใช้งานได้ดีในความชื้นสัมพัทธ์ ๑๐% - ๘๐%RH หรือดีกว่า
- มีช่องเชื่อมต่อ (Interface) แบบ VGA จำนวนไม่น้อยกว่า ๑ ช่อง
- มีช่องเชื่อมต่อ (Interface) แบบ HDMI v๒.๐ จำนวนไม่น้อยกว่า ๒ ช่อง

- จัดหาโทรทัศน์ แอล อี ดี (LED TV) แบบ Smart TV ขนาด ๕๕ นิ้ว จำนวน ๑ จอ พร้อมขาตั้งแบบล้อเลื่อน
  มีคุณลักษณะดังนี้
  - ระดับความละเอียดจอภาพ ไม่น้อยกว่า ๓๘๔๐ x ๒๑๖๐ พิกเซล
  - ขนาดจอภาพไม่น้อยกว่า ๕๕ นิ้ว
  - แสดงภาพด้วยหลอดไฟแบ็คไลท์ LED TV
  - สามารถเชื่อมต่ออินเตอร์เน็ตได้ (Smart TV)
  - เป็นระบบปฏิบัติการ Android หรือ Tizen หรือ VIDAA หรือ webOS หรืออื่น ๆ
  - ช่องต่อ HDMI ไม่น้อยกว่า ๒ ช่อง เพื่อการเชื่อมต่อสัญญาณภาพและเสียง
  - ช่องต่อ USB ไม่น้อยกว่า ๑ ช่อง รองรับไฟล์ภาพ เพลง และภาพยนต์
  - มีตัวรับสัญญาณดิจิตอล (Digital) ในตัว

- งานระบบไฟฟ้า และระบบสื่อสาร
  - ดำเนินการร้อยสายไฟในท่อร้อยสายไฟทั้งหมด
  - จัดทำ Recircuit Breaker ที่ได้มาตราฐาน
  - ติดตั้งโคมไฟ LED ขนาด ๖๐ x ๑๒๐ แบบฝังฝ้า จำนวน ๖ ชุด
  - ติดตั้งโคมไฟ Downlight แบบฝังฝ้า จำนวน ๑๒ จุด
  - ติดตั้งเต้ารับไฟฟ้า (ผนัง) จำนวน ๑๐ จุด
  - ติดตั้งเต้ารับไฟฟ้า (เดินลอย) จำนวน ๑๒ จุด
  - ติดตั้งเต้ารับไฟฟ้า (แบบ Popup) จำนวน ๑ จุด
  - ติดตั้งสายสื่อสาร (LAN) ตามที่กรมการปกครองกำหนด
  - ติดตั้งสาย HDMI ที่ใช้สำหรับ VIDEO Wall จำนวน ๘ ชุด
  - ดำเนินการย้าย Smoke Detector ตามที่กรมการปกครองกำหนด
  - ดำเนินการย้าย Sprinkler head ตามที่กรมการปกครองกำหนด

- งานระบบปรับอากาศและระบายอากาศ
  - ติดตั้งแอร์ ๔ ทิศทาง ขนาด ๒๔,๐๐๐ BTU จำนวน ๑ ตัว
    มีคุณลักษณะดังนี้
    - สามารถปรับการทำงาน (Function) ได้จากรีโมทไร้สาย ดังนี้ ปรับอุณหภูมิ, ตั้งเวลาปิดเปิด, ตั้งสวิงขึ้นลง, ปรับรูปแบบการส่งลม, ปรับแรงลม

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- ○ ต้องมีแผ่นกรองอากาศที่สามารถยับยั้งแบคทีเรีย
- ○ ระบบควบคุมต้องสามารถเปิดเครื่องใหม่อัตโนมัติหลังระบบไฟฟ้าขัดข้อง
- ○ ขนาดการทำความเย็น ๘,๙๐๐ - ๒๗,๓๐๐ BTU/Hr.
- ○ มีอัตราการหมุนเวียนอากาศ (Air Flow Rate) ๒๓/๑๘/๑๓ (H/M/L) m๓/min และ ๘๑๒ / ๖๓๕ / ๔๕๙ (H/M/L) cfm
- ○ ต้องได้รับรองมาตรฐานฉลากประหยัดไฟเบอร์ ๕
- ○ ต้องมีค่าประสิทธิภาพการทำความเย็น (SEER) ไม่น้อยกว่า ๑๘

- ติดตั้งแอร์ ๔ ทิศทาง ขนาด ๓๐,๐๐๐ BTU จำนวน ๒ ตัว มีคุณลักษณะดังนี้
  - ○ สามารถปรับการทำงาน (Function) ได้จากรีโมทไร้สาย ดังนี้ ปรับอุณหภูมิ, ตั้งเวลาปิดเปิด, ตั้งสวิงขึ้นลง, ปรับรูปแบบการส่งลม, ปรับแรงลม
  - ○ ต้องมีแผ่นกรองอากาศที่สามารถยับยั้งแบคทีเรีย
  - ○ ระบบควบคุมต้องสามารถเปิดเครื่องใหม่อัตโนมัติหลังระบบไฟฟ้าขัดข้อง
  - ○ ขนาดการทำความเย็น ๑๔,๓๐๐ - ๓๔,๑๐๐ BTU/Hr.
  - ○ มีอัตราการหมุนเวียนอากาศ (Air Flow Rate) ๒๓/๑๘/๑๓ (H/M/L) m๓/min และ ๘๑๒ / ๖๓๕ / ๔๕๙ (H/M/L) cfm
  - ○ ต้องได้รับรองมาตรฐานฉลากประหยัดไฟเบอร์ ๕
  - ○ ต้องมีค่าประสิทธิภาพการทำความเย็น (SEER) ไม่น้อยกว่า ๑๗

๕.๑.๓.๒ จ้างเหมาบริการเฝ้าระวังและวิเคราะห์ภัยคุกคามระบบสารสนเทศ (ระยะเวลา ๑๒ เดือน) และบริการการประเมินช่องโหว่ (Vulnerability Assessment) จำนวน ๓ ครั้ง ภายในระยะเวลา ๑๒ เดือน

๑) จ้างเหมาบริการเฝ้าระวังและวิเคราะห์ภัยคุกคามระบบสารสนเทศ ระยะเวลา ๑๒ เดือน) มีคุณลักษณะเฉพาะ ดังนี้

- ให้บริการตามจำนวนปริมาณข้อมูลไม่น้อยกว่า ๒๐ Gigabyte Per Day (GPD)
  - ผู้ให้บริการจะต้องจัดเก็บข้อมูล Log เป็นระยะเวลาอย่างน้อย ๙๐ วัน
  - ผู้ให้บริการจะแนะนำวิธีการตั้งค่าจัดเก็บข้อมูล (Log Source) จากระบบหรืออุปกรณ์ ตามที่ตกลงกับทางผู้รับบริการ
- ผู้ให้บริการจัดเตรียมเงื่อนไขการตรวจจับภัยคุกคาม (Correlation Rules) ให้กับผู้รับบริการ
  - ผู้ให้บริการจะออกแบบ (Correlation Rules) ให้กับองค์กรผู้รับบริการ โดยจะออกแบบเฉพาะจากข้อมูล (Log Source) ที่ได้รับและมี (MITRE)
  - ผู้ให้บริการจะเพิ่มประสิทธิภาพการตรวจจับภัยคุกคาม โดยการเพิ่มและปรับแต่ง (Correlation Rules) ตามการพัฒนา (Correlation Rules)
  - ในกรณีที่ผู้รับบริการต้องการปรับแต่ง (Correlation Rules) ให้มีความเฉพาะเจาะจงตามประสงค์ของผู้รับบริการสามารถกระทำได้โดยการร้องขอ

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- ในกรณีที่ผู้รับบริการต้องการขอปรับเปลี่ยนข้อมูลการใช้ให้มีความเฉพาะเจาะจงตามประสงค์ของผู้รับบริการสามารถกระทำได้โดยการร้องขอเพื่อปรับแต่ง (Change Request) ทั้งหมดรวมกันไม่เกิน ๕ ครั้ง/ปี

- จัดหาบุคลากรประจำสำนักบริหารการทะเบียน กรมการปกครอง คลอง ๙ ลำลูกกา แบบ ๒๔ ชั่วโมง x ๗ วัน สำหรับการเฝ้าระวัง วิเคราะห์ ตรวจจับเหตุการณ์ภัยคุกคามทางด้านไซเบอร์โดยทำการวิเคราะห์หาภัยคุกคามจากข้อมูล Log จากอุปกรณ์ที่ได้ทำการจัดเก็บ
- ผู้ให้บริการตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นและแจ้งเตือนผู้รับบริการตาม (SLA) ของประเภทภัยคุกคามที่กำหนด โดยผู้ให้บริการจำแนกประเภทภัยของคุกคาม ดังนี้
  - การเข้าใช้งานระบบโดยไม่ได้รับอนุญาต (Unauthorized Access)
  - โปรแกรมอันตรายที่มุ่งประสงค์ร้ายต่อระบบคอมพิวเตอร์ในรูปแบบใดรูปแบบหนึ่ง (Malicious Code)
  - ทราฟฟิคต้องสงสัยที่เกิดขึ้นบนระบบเครือข่าย (Suspect Traffic)
  - กิจกรรมต้องสงสัยที่เกิดขึ้นบนระบบคอมพิวเตอร์ (Suspect Activity)
  - การหลอกลวงเชิงจิตวิทยาผ่านระบบเครือข่ายสาธารณะ (Phishing Attack)
  - การค้นหาและขยายการโจมตีไปยังระบบเครือข่ายคอมพิวเตอร์ภายใน (Lateral Movement)
  - มัลแวร์เรียกค่าไถ่ (Ransomware)
  - การลักลอบหรือขโมยข้อมูล (Data Exfiltration)
  - การโจมตีเพื่อทำให้ระบบไม่สามารถดำเนินการหรือให้บริการได้ (Denial-of-Service Attack)
- ผู้ให้บริการดำเนินการจัดทำสรุปรายงานการให้บริการรายเดือน (Monthly Report) โดยรายละเอียดดังนี้
  - รายงานสรุปเหตุการณ์ภัยคุกคามทางด้านไซเบอร์ (Executive Summary Report) โดยมีรายละเอียดดังนี้
    - ระดับความรุนแรง และระดับความสำคัญ (Severity and Priority)
    - จำนวนและภาพรวมการแจ้งเตือน (Alert Summary)
    - สรุปเหตุการณ์ภัยคุกคาม (Incident Summary)
- ผู้ให้บริการดำเนินการจัดทำรายงานสรุปภาพรวมการเฝ้าระวังภัยคุกคาม (Security Posture Report) โดยมีรายละเอียดดังนี้
  - ปริมาณและลักษณะการใช้งานเครือข่าย (Traffic Statistic)
  - ลักษณะภัยคุกคามที่อุปกรณ์ความปลอดภัยตรวจจับและป้องกันได้ (Threat Summary)
  - การใช้งานหรือบริการต่างๆ ภายในองค์กร (Usage)
- ผู้ให้บริการดำเนินการจัดทำสรุปรายงานการให้บริการรายสัปดาห์ (Weekly Report)

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

- รายงานสรุปเหตุการณ์ภัยคุกคามทางด้านไซเบอร์ (Executive Summary Report) โดยมีรายละเอียด ดังนี้
  - จำนวนและภาพรวมการแจ้งเตือน (Alert Summary)
  - สรุปเหตุการณ์ภัยคุกคาม (Incident Summary)
  - สรุปภาระงานที่ได้รับการร้องขอ (Service request)

๒) จ้างเหมาบริการการประเมินช่องโหว่ (Vulnerability Assessment) จำนวน ๓ ครั้ง ภายในระยะเวลา ๑๒ เดือน
มีคุณลักษณะเฉพาะ ดังนี้

- ดำเนินการวิเคราะห์ผลการประเมินความเสี่ยงในส่วนของความปลอดภัยทางด้านระบบเครือข่าย (Network Security) โดยตรวจสอบโดยการค้นหา (Scanning) ภายในระบบโครงข่ายภายในของสำนักบริหารการทะเบียน และตรวจสอบครอบคลุมในส่วนของเครือข่ายและการสื่อสาร (Network and Communication)
  - Open Ports เช่น FTP (๒๑), Telnet (๒๓), SSH(๒๒), RDP (๓๓๘๙), SMB (๔๔๕), SNMP(๑๖๑/๑๖๒)
  - Protocol Security เช่น HTTP, Telnet
- ตรวจสอบการเปิดการเข้าถึงระยะไกลของผู้ดูแลระบบ (Remote Administrative Services - RDP, SSH, VPN)
- การสแกนหาพอร์ตและบริการที่ไม่จำเป็น (Unnecessary Services and Ports) ของ HOST Server
- ตรวจสอบช่องโหว่ในระบบปฏิบัติการ (Operating System Vulnerabilities)
- ตรวจสอบช่องโหว่ของซอฟต์แวร์ (Application and Software Vulnerabilities) และการอัปเดตแพตช์ (Patch Management)
  - Outdated Software
  - ตรวจสอบซอฟต์แวร์ที่ติดตั้งว่ามีการอัปเดตหรือหมดอายุการสนับสนุนหรือไม่
  - Third-Party Applications
  - ค้นหาช่องโหว่ในซอฟต์แวร์จากผู้พัฒนาอื่น เช่น Apache, NGINX, หรือ PHP
- ดำเนินการจัดทำรายงานและสรุปแนวทางการแก้ไขช่องโหว่ที่ตรวจพบ

๕.๒ ผู้ประสงค์จะเสนอราคาจะต้องออกแบบระบบรักษาความปลอดภัยตามข้อ ๕.๑ ให้สามารถทำงานร่วมกันได้

๖. การเปรียบเทียบคุณลักษณะเฉพาะของระบบคอมพิวเตอร์

ผู้ยื่นข้อเสนอจะต้องจัดทำตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะระบบคอมพิวเตอร์ตามที่กรมการปกครองกำหนดกับรายละเอียดเฉพาะระบบคอมพิวเตอร์ที่นำเสนอด้วยรูปแบบตาราง ดังนี้

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

ตารางเปรียบเทียบข้อเสนอโครงการจัดหาอุปกรณ์และระบบรักษาความปลอดภัย เพิ่มประสิทธิภาพด้านความมั่นคงทางเครือข่าย (Network Security)		
รายละเอียดของกรมการปกครอง	รายละเอียดของผู้ยื่นข้อเสนอ	เอกสารอ้างอิง
		ระบุหมายเลขหน้าของเอกสารอ้างอิง

๗. กำหนดเวลาส่งมอบ/สถานที่ส่งมอบ

ผู้ชนะการเสนอราคา จะต้องดำเนินการติดตั้งและส่งมอบอุปกรณ์และระบบรักษาความปลอดภัย เพิ่มประสิทธิภาพด้านความมั่นคงทางเครือข่าย (Network Security) ณ สำนักบริหารการทะเบียน คลอง ๙ อำเภอลำลูกกา จังหวัดปทุมธานี และสำนักบริหารการทะเบียน วังไชยา กรุงเทพมหานคร ให้แล้วเสร็จภายใน ๑๒๐ วัน นับถัดจากวันลงนามในสัญญา

๘. หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ

การพิจารณาใช้หลักเกณฑ์ราคาโดยพิจารณาจากราคารวม (ราคาต่ำสุด)

๙. วงเงินงบประมาณ

งบประมาณ ๙๙,๔๒๔,๐๐๐ บาท (เก้าสิบเก้าล้านสี่แสนสองหมื่นสี่พันบาทถ้วน)

๑๐. เงื่อนไขการชำระเงิน

กรมการปกครอง จะชำระเงินตามจำนวนในสัญญา โดยจะจ่ายหลังจากผู้รับจ้างปฏิบัติถูกต้องครบถ้วนตามที่กรมการปกครองกำหนดและได้ทำการตรวจรับถูกต้องเรียบร้อยแล้ว

๑๑. อัตราค่าปรับ

ค่าปรับเป็นรายวันในอัตราร้อยละ ๐.๒๐ ของราคาค่าสิ่งของที่ยังไม่ได้รับมอบต่อวัน

๑๒. การรับประกันความชำรุดบกพร่อง/ซ่อมแซมแก้ไขและการสนับสนุนการปฏิบัติงานประจำ

ผู้ยื่นข้อเสนอต้องมีความพร้อมในการสนับสนุนการใช้งาน ตลอดระยะเวลาการรับประกัน ๑ ปี นับถัดจากวันส่งมอบ ดังนี้

๑๒.๑ จัดให้มีพนักงานประจำรับแจ้งปัญหาในเวลาปฏิบัติราชการ ตั้งแต่เวลา ๐๘.๐๐ - ๑๗.๐๐ น.

๑๒.๒ ต้องมีระบบบริการรับแจ้งและติดตามการแก้ไขปัญหา (Services Web System) โดยเจ้าหน้าที่ผู้ปฏิบัติงานจะต้องสามารถแจ้งปัญหาได้ผ่านระบบดังกล่าว

๑๒.๓ ต้องมีความพร้อมในการตรวจสอบวิเคราะห์ปัญหาและดำเนินการแก้ไขปรับปรุงอุปกรณ์ที่ติดตั้งใช้งาน โดยเริ่มดำเนินการภายในวันทำการถัดไป นับตั้งแต่ได้รับแจ้งปัญหา

๑๒.๔ ในระหว่างรับประกัน ผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ ซึ่งได้ทำสัญญาซื้อขายหรือข้อตกลงเป็นหนังสือแล้วจะต้องดำเนินการตามเงื่อนไขขอบเขตของงานที่ระบุไว้ใน ข้อ ๕.๑.๓.๒ ตลอดระยะเวลา ๑๒ เดือน นับถัดจากวันที่กรมได้รับมอบสิ่งของครบถ้วน และจัดส่งรายงานผลการดำเนินงานตามข้อ ๕.๑.๓.๒ ให้กรม (ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน สำนักบริหารการทะเบียน) ทราบตามที่กำหนด หากผู้ขายไม่ดำเนินการดังกล่าวกรมมีสิทธิที่จะทำการนั้นเองหรือให้ผู้อื่นทำการนั้นแทน โดยผู้ขายต้องเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น ในการที่กรมทำการนั้นเองหรือให้ผู้อื่นทำการนั้นแทนผู้ขายไม่ทำให้ผู้ขายหลุดพ้นจากความรับผิดตามสัญญา หากผู้ขายไม่ชดใช้ค่าใช้จ่ายหรือค่าเสียหายตามที่กรมเรียกร้อง กรมมีสิทธิบังคับจากหลักประกันการปฏิบัติตามสัญญาได้

๑๓. การฝึกอบรม

ผู้ยื่นข้อเสนอจะต้องจัดฝึกอบรมเจ้าหน้าที่ผู้รับผิดชอบในการใช้งานระบบรักษาความปลอดภัย เพิ่มประสิทธิภาพด้านความมั่นคงทางเครือข่าย (Network Security) จำนวน ๑ ครั้ง ไม่น้อยกว่า ๑๐ คน รวมถึงการจัดทำคู่มือการใช้งานเป็นรูปแบบเอกสารและไฟล์อิเล็กทรอนิกส์

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

๑๔. ข้อสงวนสิทธิ์ในการพิจารณาและอื่น ๆ

๑๔.๑ ในการส่งมอบอุปกรณ์ หากภายหลังได้มีการเปลี่ยนแปลงทางเทคโนโลยีให้ดีขึ้น หรือโรงงานผู้ผลิตไม่ได้ทำการผลิตอุปกรณ์อีกต่อไป หรือผู้ผลิตไม่สามารถผลิตเพื่อส่งมอบได้ทันตามกำหนด เนื่องจากเกิดปัญหาการขาดแคลนของชิ้นส่วนอิเล็กทรอนิกส์ ทำให้ผู้ยื่นข้อเสนอจำเป็นต้องส่งมอบอุปกรณ์ต่างไปจากรายการที่นำเสนอ เพื่อให้โครงการดำเนินได้ต่อและเป็นประโยชน์ต่อทางราชการ ให้ผู้ยื่นข้อเสนอสามารถเสนออุปกรณ์ยี่ห้ออื่น/รุ่นอื่น ที่มีคุณลักษณะเทียบเท่าหรือดีกว่า เพื่อทำการพิจารณาประสิทธิภาพอุปกรณ์ที่เสนอเพื่อส่งมอบทดแทน โดยผู้ยื่นข้อเสนอไม่สามารถเรียกร้องราคาที่ตกลงผูกพันในสัญญาได้

๑๔.๒ พัสดุที่ส่งมอบนี้ต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ อยู่ในสภาพที่พร้อมใช้งานได้ทันที และมีคุณลักษณะเฉพาะตามที่กรมการปกครองกำหนด

๑๕. หน่วยงานที่รับผิดชอบ

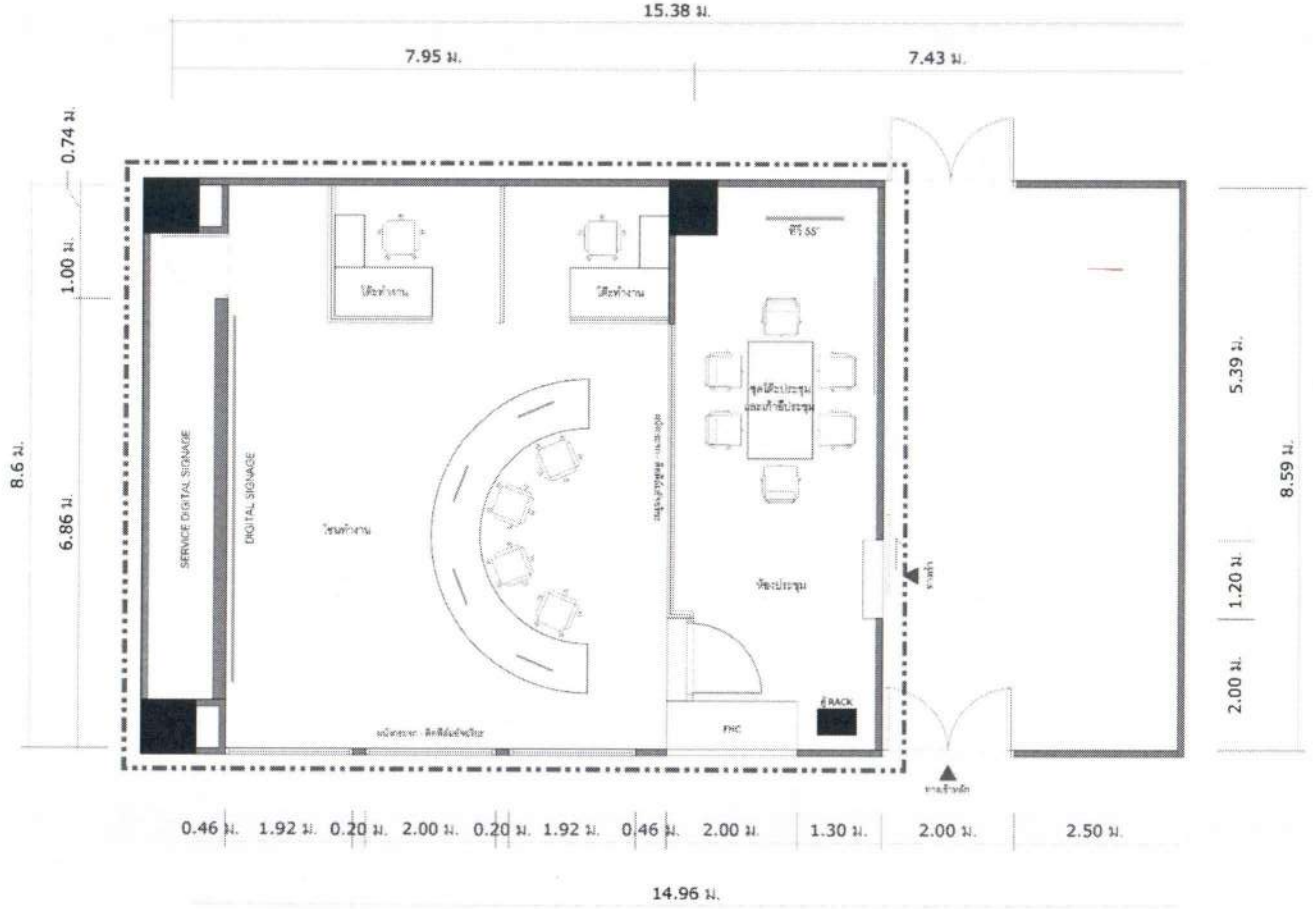
ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน สำนักบริหารการทะเบียน กรมการปกครอง

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)

ภาคผนวก ๑

แผนผังการปรับปรุงห้องศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

(BORA CIRT)



พื้นที่ดำเนินการ

(นายสิทธิโชค ชัยปัญญา) (นายรังสฤษดิ์ พรมแก้ว) (นายอภิสิทธิ์ แสงอุดม) (นายธเนตร เมืองกระจ่าง) (นายถาวร ศรีเสมอ)