

กรมสอบสวนคดีพิเศษ

ร่างขอบเขตของงาน

รายการจัดซื้อครุภัณฑ์คอมพิวเตอร์ “ระบบป้องกันการโจมตีทางไซเบอร์ และมัลแวร์ แฉวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ” จำนวน ๑ โครงการ ปีงบประมาณ พ.ศ. ๒๕๖๖

๑. ความเป็นมา

การพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารส่งผลให้เกิดการพัฒนาทั้งทางเศรษฐกิจและสังคมอย่างก้าวกระโดด ทำให้ปัจจุบันภารกิจการสืบสวนสอบสวนคดีพิเศษจึงมีความจำเป็นต้องใช้ระบบอินเทอร์เน็ตในการติดต่อประสานงานทางจดหมายอิเล็กทรอนิกส์ (Email), การสืบค้นข้อมูลข่าวสารในเครือข่าย Internet, การเฝ้าระวังและตรวจจับการกระทำผิดในเครือข่าย Internet รวมทั้งการแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น ๆ ผ่านทางเทคโนโลยี Web Service ทำให้ระบบสารสนเทศและระบบจดหมายอิเล็กทรอนิกส์ (Email) ของกรมสอบสวนคดีพิเศษ มีความเสี่ยงในการถูกโจมตีทาง Cyber จากภายนอก โดยที่ผ่านมามีกรมสอบสวนคดีพิเศษโดนโจมตีด้วย Spam Mail, Phishing Mail, Spear Phishing Mail รวมทั้งมีการโจมตีด้วย Ransomwares ผ่านทางอินเทอร์เน็ตและระบบอีเมลของกรมสอบสวนคดีพิเศษ ซึ่งทำให้เกิดความเสี่ยงต่อข้อมูลสารสนเทศที่มีความสำคัญเป็นอย่างมาก

เพื่อให้เกิดความต่อเนื่องในการพัฒนาและปรับปรุงการรักษาความปลอดภัยของระบบจดหมายอิเล็กทรอนิกส์ กรมสอบสวนคดีพิเศษ ให้มีประสิทธิภาพและปิดช่องโหว่ที่เกิดขึ้น กรมสอบสวนคดีพิเศษจึงมีความประสงค์จะจัดหาระบบป้องกันการโจมตีทางไซเบอร์และมัลแวร์ ที่มีความทันสมัยและมีประสิทธิภาพสูงในการป้องกันภัยคุกคามที่แฝงมากับ Spam Mail, Phishing Mail, Spear Phishing Mail รวมทั้งมีการโจมตีด้วย Ransomwares ผ่านทางอีเมลของกรมสอบสวนคดีพิเศษ และรองรับการให้บริการสนับสนุนการปฏิบัติการของกรมสอบสวนคดีพิเศษได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อป้องกันภัยคุกคามที่แฝงมากับ Spam Mail, Phishing Mail, Spear Phishing Mail รวมทั้งมีการโจมตีด้วย Ransomwares ผ่านทางอีเมลของกรมสอบสวนคดีพิเศษ จากการถูกโจมตีทาง Cyber

๒.๒ เพื่อให้ระบบสารสนเทศของกรมสอบสวนคดีพิเศษ มีความมั่นคงปลอดภัย และรองรับการใช้งานร่วมกับเทคโนโลยีในปัจจุบัน

๒.๓ เพื่อสนับสนุนการปฏิบัติงานในภารกิจการสืบสวนสอบสวนคดีพิเศษของกรมสอบสวนคดีพิเศษ

๓. รายการและจำนวนของพัสดุ

๓.๑ ระบบป้องกันการโจมตีทางไซเบอร์และมัลแวร์ สำหรับบริหารจัดการ จำนวน ๑ ระบบ

๓.๒ ระบบป้องกันการโจมตีทางไซเบอร์และมัลแวร์ สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวนไม่น้อยกว่า ๑,๕๐๐ ชุด (ลิขสิทธิ์)

๔. คุณสมบัติของผู้เสนอราคา

๔.๑ มีความสามารถตามกฎหมาย

๔.๒ ไม่เป็นบุคคลล้มละลาย

๔.๓ ไม่อยู่ระหว่างเลิกกิจการ

๔.๔ ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

๔.๕ ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

๔.๖ มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

๔.๗ เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

๔.๘ ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่กรมสอบสวนคดีพิเศษ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

๔.๙ ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่ รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น

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

๔.๑๑ ผู้ยื่นข้อเสนอต้องจัดทำเอกสารตารางเปรียบเทียบร่างขอบเขตของงาน **รายละเอียดตามข้อกำหนดทุกข้อ** ที่กรมสอบสวนคดีพิเศษ กำหนด กับรายละเอียดที่ผู้เสนอราคา เสนอตามตัวอย่างข้างล่าง โดยระบุเอกสารอ้างอิง แคตตาล็อก ให้ถูกต้องถ้ามีรายละเอียดใดที่แตกต่างจากข้อกำหนดจะต้องอธิบายพร้อมทั้งเปรียบเทียบข้อดีข้อเสีย ให้เข้าใจชัดเจน โดยให้ยื่นขณะเข้าเสนอราคา

ตัวอย่างตารางเปรียบเทียบ

ร่างขอบเขตของงานที่กรมสอบสวนคดีพิเศษกำหนด	ร่างขอบเขตของงานที่ผู้ยื่นข้อเสนอ เสนอ	การเปรียบเทียบ (สูงกว่า/เทียบเท่า)	เอกสารอ้างอิง (แคตตาล็อก/อื่นๆ)
๑.			
๒.			

๕. คุณลักษณะเฉพาะของพัสดุ

๕.๑ ระบบป้องกันการโจมตีทางไซเบอร์และมัลแวร์ สำหรับบริหารจัดการ จำนวน ๑ ระบบ มีคุณลักษณะอย่างน้อย ดังนี้

๕.๑.๑ ระบบป้องกันการโจมตีทางไซเบอร์และมัลแวร์ สำหรับบริหารจัดการ ต้องมีประสิทธิภาพเพียงพอต่อการใช้งานสำหรับเครื่องคอมพิวเตอร์ลูกข่าย (Endpoints) ในโครงการนี้ โดยระบบต้องสามารถทำ auto-update จาก Vendor ได้ สำหรับการอัปเดตระบบที่ติดตั้งบนเครื่องลูกข่ายให้เป็นรุ่นล่าสุดได้อย่างมีประสิทธิภาพ

๕.๑.๒ ระบบสามารถรายงานภาพรวมข้อมูลที่เกี่ยวข้องกับอุปกรณ์ที่ติดตั้ง โดยมีรายละเอียดอย่างน้อยดังนี้ IP address, MAC Address, ผู้ใช้ที่ใช้งานอยู่, ผู้ใช้งานที่ล็อกอิน, นโยบายที่ใช้งานอยู่, กลุ่มอุปกรณ์, ระบบปฏิบัติการที่ติดตั้งบนอุปกรณ์และชื่ออุปกรณ์

๕.๑.๓ สามารถเข้าใช้งานผ่านเว็บเบราว์เซอร์ ได้แก่ Microsoft Edge, Google Chrome, Mozilla Firefox เป็นอย่างน้อย

๕.๑.๔ สามารถทำนโยบายแบ่งแยกตามแผนกได้ (Group Policy)

- ๕.๑.๕ รองรับ Role Based Administration (RBA) สามารถที่จะเปิดช่องทางในการบริหาร ขั้นตอนการเข้าถึงได้จากหลายชั้น (Level of Access) ตัวอย่างเช่น Master Administrator, Administrator, Read Only และ IT Administrator ได้
 - ๕.๑.๖ สามารถใช้งานร่วมกับ Active Directory
 - ๕.๑.๗ สามารถทำการ Whitelist (Allow List) ของไฟล์ต่าง ๆ ได้ โดยการใช้ค่า Hash, Certificate หรือใช้ตำแหน่งที่ตั้งของไฟล์ เป็นตัวกำหนดได้
 - ๕.๑.๘ สามารถทำการ Blacklist (File Hash Deny List) ของไฟล์ต่าง ๆ ได้ โดยการใช้ค่า Hash ของไฟล์ เป็นตัวกำหนดได้
 - ๕.๑.๙ สามารถรองรับการทำงานนโยบายแบ่งแยกตามแผนกได้ และนำข้อมูลออกมาในรูปแบบของ ไฟล์ excel หรือ CSV ได้
 - ๕.๑.๑๐ สามารถรองรับการบริหารแบบ Group โดยจัดแยก Devices ตาม Policy ที่ต้องการ ได้
 - ๕.๑.๑๑ สามารถบริหารเครื่องลูกข่ายปลายทาง Endpoint ทุกเครื่องที่ติดตั้งในหน้าบริหาร จัดการส่วนกลาง Centralized Management Console
 - ๕.๑.๑๒ สามารถตั้งค่าการแจ้งเตือนได้
 - ๕.๑.๑๓ สามารถแก้ไขไฟล์, ลบไฟล์, บังคับใช้นโยบาย, ทำการ Isolation เครื่องลูกข่ายจาก ส่วนกลางได้
 - ๕.๑.๑๔ สามารถรองรับการรวบรวมข้อมูลเพื่อจัดเก็บไปยังระบบเก็บข้อมูลส่วนกลาง (Syslog Server) หรือระบบปฏิบัติการของ SIEM (Security Information and Event Management) ได้ โดยการทำงานนั้นสามารถถ่ายทอดข้อมูลให้กับโปรโตคอลหลาย รูปแบบเช่น (UDP, TCP และ TLS over TCP) และสามารถรองรับการทำงานคละ รูปแบบของ Syslog Format ในรูปแบบของ LEEF, RFC๕๔๒๔ เพื่อการทำงาน ร่วมกันได้
 - ๕.๑.๑๕ สามารถส่งข้อมูลเพื่อทำการตรวจสอบเหตุการณ์ Audit Log Events ในระบบไปยัง ระบบเก็บข้อมูลส่วนกลาง (Syslog) ได้
 - ๕.๑.๑๖ สามารถส่งข้อมูลและเหตุการณ์ Security Events ไปยังระบบเก็บข้อมูลส่วนกลาง (Syslog) ได้
 - ๕.๑.๑๗ สามารถแสดง MITRE Mapping ตามเหตุการณ์ที่เกิดขึ้นได้ โดยสรุปข้อมูลในรูปแบบ ของ Tactic, Technique และ Sub-Technique ได้
 - ๕.๑.๑๘ สามารถแบ่งการจัดการในรูปแบบ Multi Tenant เพื่อให้สามารถแสดงข้อมูลได้ทั้ง โดยรวมทั้งองค์กรและแยกเป็นหน่วยย่อยได้ โดยที่ทางส่วนกลางสามารถบริหารจัดการ ดูแลภาพรวมทั้งหมดและดูแลแต่ละหน่วยหรือสาขาได้อย่างชัดเจน
- ๕.๒ ระบบป้องกันการโจมตีทางไซเบอร์และมัลแวร์ สำหรับเครื่องคอมพิวเตอร์ลูกข่าย จำนวนไม่น้อย กว่า ๑,๕๐๐ ชุด (ลิขสิทธิ์) มีคุณลักษณะอย่างน้อย ดังนี้
- ๕.๒.๑ เป็นระบบที่ใช้เทคโนโลยีการตรวจจับแบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในรูปแบบ Deep learning สามารถรองรับการการป้องกันภัยคุกคามจากภายใน เครือข่ายโดยไม่ต้องพึ่งการทำ Daily Update โปรแกรม

/๕.๒ สามารถ...

- ๕.๒.๒ สามารถติดตั้งลงบนเครื่องคอมพิวเตอร์โดยใช้ไฟล์ในรูปแบบของ Installation Executable โดยใช้พื้นที่ติดตั้งไม่เกิน ๕๐๐ MB
- ๕.๒.๓ ใช้หน่วยความจำ (Memory) ของเครื่องคอมพิวเตอร์ และทรัพยากรของหน่วยประมวลผลกลาง(CPU) น้อยกว่าร้อยละ ๑๐ ในสถานะตรวจจับและเฝ้าระวัง
- ๕.๒.๔ รองรับการป้องกันภัยคุกคาม Malware ต่างๆ แบบ Real-Time ได้ โดยไม่จำเป็นต้องที่จะต้องมี การ อัปเดต Signature ใด ๆ ทั้งสิ้น
- ๕.๒.๕ สามารถป้องกันภัยคุกคามที่บุกรุกเข้ามาในรูปแบบของไฟล์ที่หลากหลายในรูปแบบของ Executable Files, PDFs, ไฟล์งานของ Microsoft Office Files, Archive Files ได้
- ๕.๒.๖ สามารถทำการตรวจสอบอย่างเต็มรูปแบบ (Full Scan) ในช่วงหลังจากการติดตั้ง (Installation) เพื่อที่จะวินิจฉัยและแยกแยะโปรแกรมประสงค์ร้ายต่าง ๆ (Malware) ที่อาจจะมีอยู่ในเครื่อง คอมพิวเตอร์ได้
- ๕.๒.๗ สามารถแยกแยะภัยคุกคามส่วนมากได้ โดยจะจัดเป็นรูปแบบ Deep Classification เช่น Ransomware, Backdoor, Dropper เป็นอย่างน้อย โดยไม่จำเป็นต้องส่งข้อมูลต่อให้กับ ๓rd Party และสามารถแสดงข้อมูลของ Process Chain ได้
- ๕.๒.๘ สามารถแยกแยะภัยคุกคามส่วนมากได้ โดยจะจัดเป็นรูปแบบ Deep Classification หรือ Threat Type เช่น Ransomware, Backdoor, Dropper เป็นอย่างน้อย โดยไม่จำเป็นต้องส่งข้อมูลต่อให้กับ ๓rd Party และสามารถแสดงข้อมูลของ Process Chain ได้
- ๕.๒.๙ รองรับการติดตั้งภายในระบบปฏิบัติการดังต่อไปนี้เป็นอย่างน้อย
- (๑) Window ๗ SP๑ (๓๒-bit, ๖๔-bit)
 - (๒) Window ๘ (๓๒-bit, ๖๔-bit)
 - (๓) Window ๘.๑ (๓๒-bit, ๖๔-bit)
 - (๔) Window ๑๐ (๓๒-bit, ๖๔-bit)
 - (๕) Window ๑๑ (๖๔-bit)
 - (๖) Windows Server ๒๐๐๘ R๒ SP๑(๖๔-bit)
 - (๗) Windows Server ๒๐๑๒ (๖๔-bit)
 - (๘) Windows Server ๒๐๑๒ R๒ (๖๔-bit)
 - (๙) Windows Server ๒๐๑๖ (๖๔-bit)
 - (๑๐) Windows Server ๒๐๑๙ (๖๔-bit)
- ๕.๒.๑๐ สามารถตรวจจับมัลแวร์ในรูปแบบ Pre-execution Prevention ได้ไม่น้อยกว่า ๙๐% จากจำนวนไฟล์มัลแวร์ทั้งหมดที่ทดสอบ โดยนำระบบมาทดสอบการตรวจจับมัลแวร์กับกรมสอบสวนคดีพิเศษในวันส่งมอบ (มัลแวร์ที่ใช้ทดสอบจากเว็บ ๓rd Party เช่น VIRSTOTAL เป็นต้น)
- ๕.๒.๑๑ สามารถตรวจจับและยับยั้งมัลแวร์ในรูปแบบออฟไลน์หรือในขณะที่เครื่องลูกข่ายไม่สามารถเชื่อมต่ออินเทอร์เน็ตได้เป็นอย่างดีมีประสิทธิภาพ โดยสามารถป้องกันภัยคุกคามได้ไม่น้อยกว่า ๗๕% จากจำนวนไฟล์มัลแวร์ทั้งหมดที่ทดสอบ โดยนำระบบมาทดสอบการตรวจจับมัลแวร์กับกรมสอบสวนคดีพิเศษในวันส่งมอบ (มัลแวร์ที่ใช้ทดสอบจากเว็บ ๓rd Party เช่น VIRSTOTAL เป็นต้น)

- ๕.๓ ผู้เสนอราคาจะต้องให้การสนับสนุนช่วยเหลือทางเทคนิค ความสามารถในการติดตั้ง และการบริการหลังการขายสำหรับโครงการนี้ เพื่อให้การติดตั้งใช้งานเป็นไปอย่างมีประสิทธิภาพ
- ๕.๔ ผลิตรถยนต์ที่เสนอจะต้องเป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน และยังอยู่ในสายการผลิต

๖. ระยะเวลาการส่งมอบพัสดุ

กำหนดการส่งมอบพัสดุภายใน ๑๕๐ วัน นับถัดจากวันที่ผู้ขาย/ผู้รับจ้าง ลงนามในสัญญาซื้อขาย

๗. หลักเกณฑ์การพิจารณา

ใช้เกณฑ์ราคา

๘. การจ่ายเงิน

กรมสอบสวนคดีพิเศษ จะชำระเงินให้ผู้ขายหรือผู้รับจ้าง เมื่อผู้ขายหรือผู้รับจ้างได้ส่งมอบพัสดุครบถ้วนถูกต้องตามใบสั่งซื้อ/ใบสั่งจ้าง/สัญญาซื้อขาย และคณะกรรมการตรวจรับพัสดุได้ตรวจรับพัสดุไว้ในราชการเรียบร้อยแล้ว

๙. การรับประกันความชำรุดบกพร่อง

ผู้ยื่นข้อเสนอ ต้องรับประกันเป็นระยะเวลาไม่น้อยกว่า ๑ ปี โดยเข้ามาทำการแก้ไข/ซ่อมแซม ณ ที่ตั้ง และให้บริการแบบ (On-site Service) หรือ Remote Support นับถัดจากวันที่คณะกรรมการตรวจรับพัสดุได้มีมติตรวจรับพัสดุถูกต้องครบถ้วนแล้ว หรือตามที่สัญญากำหนด

๑๐. การคิดค่าปรับ

การคิดค่าปรับให้เป็นไปตามข้อกำหนดในสัญญา

๑๑. ข้อกำหนดอื่น ๆ

๑๑.๑ ผู้ชนะการเสนอราคาต้องแจ้งรายชื่อเจ้าหน้าที่ที่เป็นผู้รับผิดชอบในการสนับสนุนให้คำปรึกษาในการวิเคราะห์ แก้ไขปัญหาและประสานงานโครงการให้ชัดเจน ตลอดอายุสัญญาจนสิ้นระยะเวลารับประกัน

๑๑.๒ ผู้เสนอราคาจะต้องส่งมอบรายละเอียดรายการทั้งหมด โดยจะต้องมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย ได้แก่ ๑. ยี่ห้อ ๒. บริษัทผู้ผลิต ๓. หมายเลขผลิตภัณฑ์ (Serial No.) หรือ หมายเลขชุดโปรแกรม ฯลฯ (ข้อมูลตามที่มีจริง) โดยส่งมอบเป็น ไฟล์ Excel และไฟล์ PDF และเอกสาร ในวันส่งมอบ

๑๑.๓ การกระทำใด ๆ อันจะก่อให้เกิดความเสียหายต่อระบบของกรมสอบสวนคดีพิเศษ จะต้องแจ้งและได้รับอนุญาตจากเจ้าหน้าที่ผู้รับผิดชอบของกรมสอบสวนคดีพิเศษก่อน

๑๑.๔ ผลเสียหายที่เกิดขึ้นจากการกระทำใด ๆ ของผู้เสนอราคา ผู้เสนอราคาต้องรับผิดชอบการกระทำนั้น ๆ ทั้งหมด

๑๒. การฝึกอบรมและคู่มือการใช้งาน

๑๒.๑ ผู้เสนอราคาต้องจัดฝึกอบรมให้เจ้าหน้าที่ผู้ดูแลระบบของกรมสอบสวนคดีพิเศษ จำนวนไม่น้อยกว่า ๔ คน เป็นระยะเวลาไม่น้อยกว่า ๖ ชั่วโมง โดยมีเนื้อหาครอบคลุมถึงระบบป้องกันการโจมตีทางไซเบอร์ และมัลแวร์ ที่ส่งมอบให้กับกรมสอบสวนคดีพิเศษ รวมทั้งการดูแลบำรุงรักษาระบบได้อย่างมีประสิทธิภาพ และรับผิดชอบค่าใช้จ่ายในการฝึกอบรมทั้งหมด

๑๒.๒ ผู้เสนอราคาต้องส่งมอบคู่มือการใช้งานระบบป้องกันการโจมตีทางไซเบอร์ และมัลแวร์ จำนวนไม่น้อยกว่า ๔ ชุด และในรูปแบบไฟล์ PDF ให้กับกรมสอบสวนคดีพิเศษในวันที่ส่งมอบ

๑๓. ลิขสิทธิ์โปรแกรม

๑๓.๑ ผู้เสนอราคาต้องส่งมอบลิขสิทธิ์การใช้งานโปรแกรมหรือซอฟต์แวร์หรือระบบที่จัดซื้อในโครงการนี้ทั้งหมด ให้เป็นลิขสิทธิ์การใช้งานของกรมสอบสวนคดีพิเศษ

๑๓.๒ ในกรณีที่บุคคลภายนอกกล่าวอ้าง หรือใช้สิทธิเรียกร้องใด ๆ ว่ามีการละเมิดลิขสิทธิ์ หรือสิทธิบัตรเกี่ยวกับ ระบบป้องกันการโจมตีทางไซเบอร์ และมัลแวร์ ปิงบประมาณ พ.ศ. ๒๕๖๖ ตามสัญญาฉบับนี้ โดยผู้ซื้อไม่ได้แก้ไขตัดแปลงไปจากเดิม ผู้ขายจะต้องดำเนินการตั้งปวง เพื่อให้การกล่าวอ้าง หรือเรียกร้องดังกล่าวระงับสิ้นไปโดยเร็ว หากผู้ขายมีอำนาจกระทำได้และผู้ซื้อต้องรับผิดชอบใช้ค่าเสียหายต่อบุคคลภายนอก เนื่องจากผลแห่งการละเมิดลิขสิทธิ์หรือสิทธิบัตรดังกล่าว ผู้ขายต้องชำระค่าเสียหายและค่าใช้จ่าย รวมทั้งค่าฤชาธรรมเนียม และค่าทนายความแทนผู้ซื้อ ทั้งนี้ผู้ซื้อจะแจ้งผู้ขายให้ทราบเป็นลายลักษณ์อักษรในการกล่าวอ้างหรือเรียกร้องดังกล่าว

- คณะกรรมการกำหนดร่างขอบเขตของงาน ตามคำสั่งกรมสอบสวนคดีพิเศษที่ ๘๗๙/๒๕๖๕ ลงวันที่ ๒๓ สิงหาคม พ.ศ. ๒๕๖๕

ลงชื่อ.....ประธานคณะกรรมการฯ
(นายพัลลภ เกิดเทพ)
พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ

ลงชื่อ.....กรรมการ
(นายพงษ์บัณฑิต ชัยชาญ)
เจ้าหน้าที่คดีพิเศษชำนาญการ

ลงชื่อ.....กรรมการ
(นายพัทธดนย์ ตันติภักดิ์)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ