ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์

ประจำปีงบประมาณ พ.ศ.๒๕๖๙

โครงการเฝ้าระวังตรวจสอบและแจ้งเตือนความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

กรมป่าไม้ กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	แบบ: ICT-MGNT๐๑-F๐๑
	** เข้าสู่การพิจารณาของคณะอนุกรรมการฯ ครั้งที่ ...๑.../๒๕๖๘	งบประมาณเกิน ๕ ล้านบาท

ก. ข้อมูลทั่วไป

๑. ชื่อโครงการ

โครงการเฝ้าระวังตรวจสอบและแจ้งเตือนความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

๒. ส่วนราชการ / รัฐวิสาหกิจ

๒.๑ ชื่อหน่วยงาน	กรมป่าไม้	
๒.๒ หัวหน้าส่วนราชการ	ชื่อ: นายสุรชัย อจลบุญ	โทร: ๐ ๒๕๖๑ ๔๒๙๒-๓ ต่อ ๕๑๗๓
	ตำแหน่ง : อธิบดีกรมป่าไม้	e-mail: surachai๒๙p@hotmail.com
๒.๓ DCIO	ชื่อ: นายนิกร ศิรโรจนานนท์	โทร: ๐ ๒๕๖๑ ๔๒๙๒ ต่อ ๕๑๗๑
	ตำแหน่ง: รองอธิบดีกรมป่าไม้	e-mail: nikorn.sira@gmail.com
๒.๔ ผู้รับผิดชอบโครงการ	ชื่อ: นายสัมพันธ์ มีสิทธิ์	โทร: ๐๒๕๖๑๔๒๙๒ต่อ ๕๗๕๔
	ตำแหน่ง: ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	e-mail: samphanmeesith@gmail.com

๓. วงเงินงบประมาณ ปี พ.ศ. ๒๕๖๙

๓.๑ งบประมาณรวม	(ตัวเลข) ๔๒,๘๕๐,๙๗๐ บาท	
	(ตัวอักษร) สี่สิบสองล้านแปดแสนห้าหมื่นเก้าร้อยเจ็ดสิบบาทถ้วน	
๓.๒ งบประมาณในการจัดหาระบบคอมพิวเตอร์	(ตัวเลข) ๔๒,๘๕๐,๙๗๐ บาท	
	(ตัวอักษร) สี่สิบสองล้านแปดแสนห้าหมื่นเก้าร้อยเจ็ดสิบบาทถ้วน	
๓.๓ อำนาจการอนุมัติโครงการ	☑ คณะกรรมการบริหารฯ (กระทรวง)	☐ กระทรวง DE (วงเงินมากกว่า ๑๐๐ ล้านบาท)
๓.๔ แหล่งเงิน	☑ งบประมาณประจำปี	☐ เปลี่ยนแปลงรายการ/เงินเหลือจ่าย
	☐ เงินรายได้	☐ เงินช่วยเหลือ / เงินนอกงบประมาณ
	☐ อื่นๆ (ระบุ)	

๔. วิธีการจัดหา

☑ จัดซื้อ	☐ การจ้าง	☐ การจ้างที่ปรึกษา
☐ การจ้างออกแบบและควบคุมงาน	☐ การแลกเปลี่ยน	☐ การเช่า

๕. ลักษณะโครงการ

๕.๑ ☐ พัฒนาระบบ	☐ มีเอกสารแบบบัญชีราคากลาง ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีเหตุผลประกอบในข้อ ข. ๔.๓ (กรณีมีใบเสนอราคาไม่ครบ ๓ ผู้ประกอบการ)
๕.๒ ☐ ระบบกล้องโทรทัศน์วงจรปิด (CCTV)	☐ ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (รายการที่.....) ☐ ไม่ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผลิตภัณฑ์ (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผลิตภัณฑ์ (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีเหตุผลประกอบในข้อ ข. ข้อ ๔.๓ (กรณีมีใบเสนอราคาไม่ครบ ๓ ผลิตภัณฑ์ / ๓ ผู้ประกอบการ)

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	แบบ: ICT-MGNT๐๑-F๐๑
	** เข้าสู่การพิจารณาของคณะอนุกรรมการฯ ครั้งที่ ...๑/๒๕๖๘	งบประมาณเกิน ๕ ล้านบาท

๕.๓ ☑ จัดซื้อครุภัณฑ์ / โปรแกรม	☐ ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (รายการที่.....) ☑ ไม่ตรงตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (รายการที่..๑-๘.....) ☑ มีใบเสนอราคาจำนวน ๓ ผลิตภัณฑ์ (รายการที่.....๑-๘.....) ☐ มีใบเสนอราคาจำนวน_____ผลิตภัณฑ์ (รายการที่.....) ☑ มีใบเสนอราคาจำนวน ๓ ผู้ประกอบการ (รายการที่.....๑-๘.....) ☐ มีใบเสนอราคาจำนวน_____ผู้ประกอบการ (รายการที่.....) ☐ มีเหตุผลประกอบในข้อ ข. ข้อ ๔.๓ (กรณีมีใบเสนอราคาไม่ครบ ๓ ผลิตภัณฑ์ / ๓ ผู้ประกอบการ)

๖. การจัดหา

๖.๑	☐ ขยายระบบเดิม / ต่อเนื่อง	☑ จัดหาใหม่	
๖.๒	☑ โครงการตามแผนยุทธศาสตร์/บูรณาการ	☑ โครงการตามภารกิจพื้นฐาน	☐ โครงการตามแนวพระราชดำริ
	☐ โครงการตามแผนพัฒนาจังหวัด/กลุ่มจังหวัด	☐ โครงการตามข้อสั่งการ	
	☐ อื่นๆ (ระบุ).....		
๖.๓	☐ Cloud	☐ Big Data	☐ Data Center
	☐ ทดแทนของเดิม	☑ เพิ่มประสิทธิภาพระบบ	☐ งานวิจัย

๗. ลักษณะการจัดหาตามเงื่อนไขที่กระทรวง DE กำหนด

ข้อ ๑) การจัดหาที่หน่วยงานสามารถดำเนินการได้เอง (มูลค่าไม่เกิน ๑๐๐ ล้านบาท)

☐ ๑.๑) เป็นการจัดหาครุภัณฑ์คอมพิวเตอร์และโปรแกรมสำนักงานพื้นฐาน ตามคุณสมบัติและราคามาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด ภายใต้เงื่อนไขในการใช้งานคอมพิวเตอร์ไม่เกิน ๑ เครื่อง / คน โดยเฉลี่ย ตามความเหมาะสมกับภารกิจของหน่วยงาน

☐ ๑.๒) เป็นการจัดหาระบบคอมพิวเตอร์เพื่อทดแทนระบบที่ใช้มาแล้วไม่น้อยกว่า ๕ ปี (จัดหาได้ในวงเงินไม่มากกว่าเดิม และให้วงเงินที่ขอครอบคลุมถึงการถ่ายโอนข้อมูลด้วย)

☑ ๑.๓) เป็นการจัดหาระบบคอมพิวเตอร์เพื่อเพิ่มศักยภาพของระบบ ตามงาน / แผนงาน / โครงการเดิม โดยระบบงานดังกล่าวไม่มีความซ้ำซ้อน / เชื่อมโยง / สัมพันธ์กับงานในภารกิจของหน่วยงานอื่น

☐ ๑.๔) รัฐวิสาหกิจสามารถจัดหาระบบคอมพิวเตอร์ได้โดยไม่ต้องขอความเห็นชอบจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ข้อ ๒) การจัดหาต้องขอความเห็นชอบต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (มูลค่าเกิน ๑๐๐ ล้านบาท)

☐ ๒.๑) เป็นการจัดหาระบบคอมพิวเตอร์งาน / แผนงาน / โครงการที่นอกเหนือจากข้อ ๑.

☐ ๒.๒) เป็นการปรับปรุงเปลี่ยนแปลงโครงการตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ให้ความเห็นชอบแล้ว (ต้องขอความเห็นชอบใหม่)

☐ เป็นหน่วยงานที่ได้รับการยกเว้นการปฏิบัติตามหลักเกณฑ์ฯ เนื่องจากยุทธศาสตร์ของกระทรวงได้รับความเห็นชอบจากคณะรัฐมนตรี และได้ลงนามในคำรับรองการปฏิบัติราชการแล้ว โดยให้กระทรวงฯ ดำเนินการพิจารณาอนุมัติการจัดหาระบบฯ ของหน่วยงานในสังกัดได้เอง (มติคณะรัฐมนตรี ๒๓ มีนาคม ๒๕๔๗)

หมายเหตุ โปรดดูรายละเอียด / เงื่อนไขการดำเนินงาน และการรายงานที่เกี่ยวเนื่อง ได้เพิ่มเติมใน หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุดที่ ๐๕๐๔/๔๙๕๖ ลงวันที่ ๓๑ มีนาคม ๒๕๔๗ เรื่อง หลักเกณฑ์และแนวทางปฏิบัติการจัดหาระบบคอมพิวเตอร์ของรัฐ

ข. ข้อมูลโครงการ

๑. หลักการและเหตุผลความเป็นมาของโครงการ

กรมป่าไม้ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานซึ่งทำหน้าที่ในการพัฒนาระบบสารสนเทศ ระบบฐานข้อมูล ระบบภูมิศาสตร์สารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ ตลอดจนการให้บริการระบบเครือข่ายอินเตอร์เน็ต การประชุมออนไลน์ (Video Conference) และการติดต่อสื่อสารด้านเทคโนโลยีสารสนเทศในรูปแบบต่างๆ แก่บุคลากรของกรมป่าไม้ ประชาชน และผู้ประกอบการ ให้สามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว มีประสิทธิภาพ ถูกต้อง อีกทั้งยังมีการใช้บริการการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ เช่น กรมการปกครอง กรมศุลกากร สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน) กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น ซึ่งบริการดังข้างต้นที่ได้กล่าวมาเป็นระบบเทคโนโลยีสารสนเทศหลักของกรมป่าไม้ เพื่อพัฒนาไปสู่นโยบายไทยแลนด์ ๔.๐ และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย

ปัจจุบันอุปกรณ์ และซอฟต์แวร์ที่ใช้ในการป้องกันภัยคุกคามทางด้านไซเบอร์ของกรมป่าไม้ ไม่มีประสิทธิภาพเพียงพอต่อการป้องกันภัยคุกคามทางไซเบอร์ที่มีรูปแบบการโจมตีแบบใหม่ๆ เช่น การติดไวรัส WannaCry ransomware การติดไวรัส Botnet และการถูกเจาะระบบสารสนเทศของกรมป่าไม้ โดยมีระบบสารสนเทศที่ถูกเจาะระบบแล้ว จำนวน ๓ ระบบ ๑) ระบบข้อมูลสารสนเทศกรมป่าไม้ (forestinfo.forest.go.th) ๒) ลงทะเบียนต้นไม้ในที่ดินกรรมสิทธิ์ (etree.forest.go.th) และ ๓) ระบบภูมิสารสนเทศเพื่อการบริหารกรมป่าไม้ (gis.forest.go.th) โดยก่อให้เกิดความเสียหายต่อข้อมูลและชื่อเสียงกรมป่าไม้ ประกอบกับเพื่อให้เป็นไปตามข้อกำหนดตามหลักเกณฑ์ของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. วัตถุประสงค์ของโครงการ

๑. เพื่อจัดหาระบบป้องกันภัยคุกคามระบบสารสนเทศและระบบเครือข่าย
๒. เพื่อป้องกันไวรัส WannaCry ransomware ไวรัส Botnet และการถูกเจาะระบบสารสนเทศของกรมป่าไม้
๓. เพื่อเพิ่มประสิทธิภาพการค้นหาและวิเคราะห์ภัยคุกคามที่เกิดขึ้นในระบบเครือข่ายให้สามารถค้นหา และแจ้งเตือนได้อย่างรวดเร็ว
๔. เพื่อตรวจหาช่องโหว่ที่เกิดขึ้นในระบบเครือข่ายและระบบสารสนเทศ
๕. เพื่อให้เป็นไปตามข้อกำหนดตามหลักเกณฑ์ของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในหมวดหมู่ของการป้องกัน

๓. เป้าหมายของโครงการ

๑. มีระบบป้องกันภัยคุกคามระบบสารสนเทศและเครือข่าย ที่มีความสามารถในการป้องกันภัยคุกคามประเภทใหม่ๆ เช่น ไวรัส WannaCry ransomware ไวรัส Botnet และป้องกันการถูกเจาะระบบสารสนเทศของกรมป่าไม้

๒. มีระบบการค้นหา วิเคราะห์ แจ้งเตือนภัยคุกคามที่เกิดขึ้นได้ได้อย่างรวดเร็ว และมีความสามารถในการสร้างกฎ (Policy) การปิดกั้น (Block) ภัยคุกคามที่ตรวจพบได้โดยอัตโนมัติ

๓. ระบบสารสนเทศและระบบเครือข่ายของกรมป่าไม้มีความมั่นคงปลอดภัย

๔. สภาพพื้นฐานก่อนเริ่มโครงการ (Project Baseline Data)

๔.๑ สถานภาพพื้นฐานโดยทั่วไป

๑) มีอุปกรณ์ป้องกันเครือข่าย (Firewall) แต่ไม่เพียงพอต่อการป้องกันภัยคุกคามใหม่ๆ ที่เกิดขึ้นได้

๒) มีโปรแกรมป้องกันไวรัส สำหรับเครื่องแม่ข่าย จำนวน ๕ ชุด และสำหรับเครือข่ายลูกข่าย จำนวน ๑๙๐ ชุด ซึ่งไม่เพียงพอต่อจำนวนเครื่องลูกข่ายที่มีอยู่ในปัจจุบันที่ประมาณ ๘๐๐ เครื่อง

๓) ระบบสารสนเทศของกรมป่าไม้ถูกเจาะระบบแล้ว จำนวน ๓ ระบบ ๑) ระบบข้อมูลสารสนเทศกรมป่าไม้ (forestinfo.forest.go.th) ๒) ลงทะเบียนต้นไม้ในที่ดินกรรมสิทธิ์ (etree.forest.go.th) และ ๓) ระบบภูมิสารสนเทศเพื่อการบริหารกรมป่าไม้ (gis.forest.go.th)

๔. สภาพพื้นฐานก่อนเริ่มโครงการ (Project Baseline Data)

๔.๒ สภาพปัญหาของผู้รับบริการ ผู้เกี่ยวข้องที่มีส่วนได้ส่วนเสีย ตลอดจนผู้ประกอบการเอกชนหรือประชาชนโดยรวม (ถ้ามี)

ระบบสารสนเทศของกรมป่าไม้มีความเสี่ยงที่จะถูกเจาะระบบได้ ซึ่งจะสร้างความเสียหายอย่างใหญ่หลวง เช่น ทำลายข้อมูล หรือเปลี่ยนแปลงข้อมูล หรือนำข้อมูลที่ได้ไปจำหน่าย หรือการละเมิดข้อมูลส่วนบุคคล โดยจะสร้างความเสียหายต่อประชาชนและผู้ประกอบการ

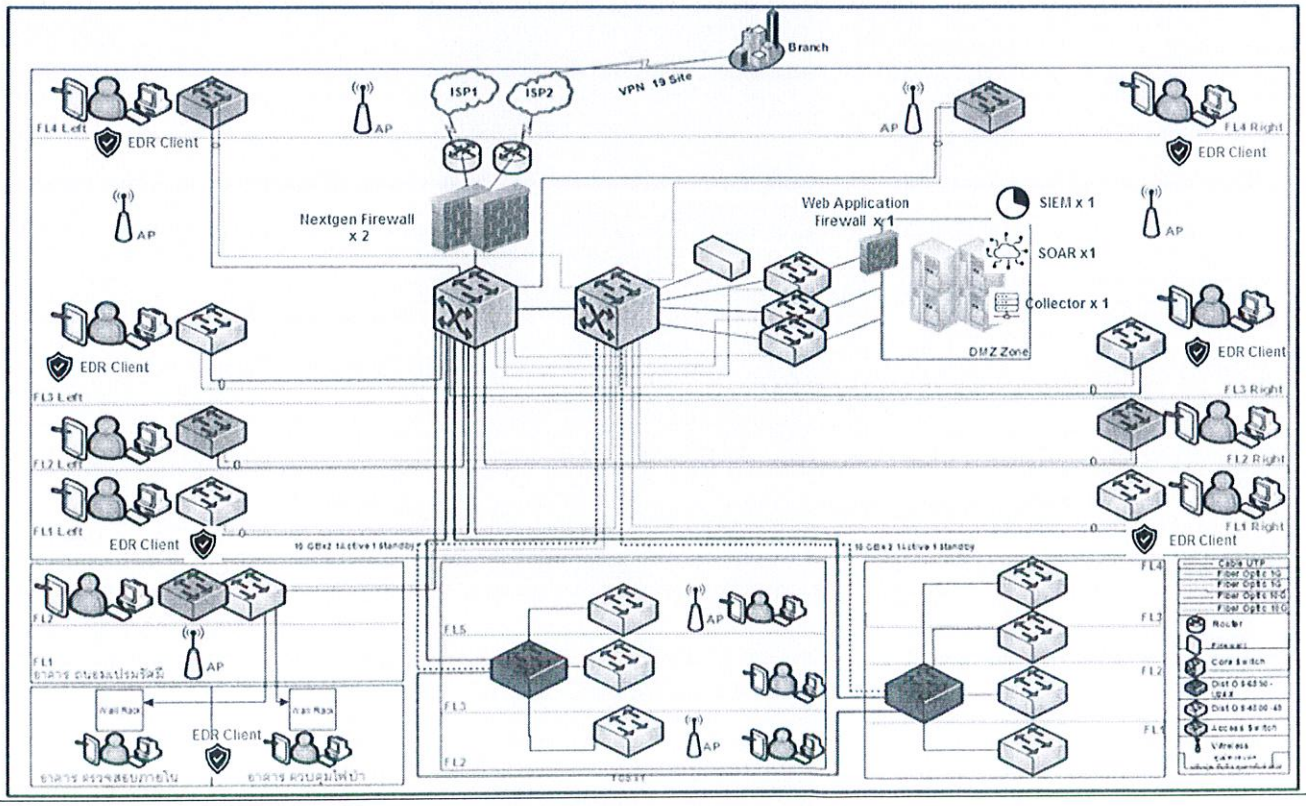
๔.๓ ปัญหาอุปสรรคในการปฏิบัติงาน/เหตุผลความจำเป็นที่ต้องจัดหาครั้งนี้

ปัจจุบันอุปกรณ์และเทคโนโลยีที่ใช้ในการป้องกันภัยคุกคามทางด้านไซเบอร์ที่มีอยู่ของกรมป่าไม้ มีจำนวนไม่เพียงพอ ประกอบกับมีภัยคุกคามทางไซเบอร์ที่มีรูปแบบการโจมตีแบบใหม่ๆ ซึ่งอุปกรณ์ที่มีอยู่ไม่สามารถป้องกันภัยคุกคามได้ ซึ่งเป็นเหตุให้ผู้ไม่ประสงค์ดี (Hacker) สามารถโจมตีระบบสารสนเทศที่สำคัญของกรมป่าไม้ ซึ่งจะก่อให้เกิดความเสียหายแก่หน่วยงานได้ กรมป่าไม้จึงมีความจำเป็นอย่างยิ่งในการดำเนินการโครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

๔.๔ ระบบหรืออุปกรณ์ทั้งหมดที่มีอยู่ในปัจจุบันของหน่วยงาน

รายการ	สถานที่ติดตั้ง/ชื่อระบบงาน	ติดตั้งเมื่อปี พ.ศ.
อุปกรณ์กระจายสัญญาณหลัก (Core Switch)	ห้อง Data Center	๒๕๖๔
อุปกรณ์ป้องกันเครือข่าย (Firewall Fortigate)	ห้อง Data Center	๒๕๖๒
อุปกรณ์กระจายสัญญาณย่อย (Distribution switch)	ห้อง Data Center	๒๕๕๙
อุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless)	ห้อง Data Center	๒๕๕๙
อุปกรณ์ควบคุมสัญญาณเครือข่ายไร้สาย (Wireless Controller)	ห้อง Data Center	๒๕๕๙
อุปกรณ์แจกหมายเลขไอพีแอสเดรส (Infoblox)	ห้อง Data Center	๒๕๕๙
อุปกรณ์สำรองไฟฟ้าขนาด ๒๐ KVA	ห้อง Data Center	๒๕๖๕

๔.๕ ผังโครงสร้างเครือข่ายคอมพิวเตอร์ของหน่วยงานและ/หรือแผนผังโครงการตามข้อ ๑. (ถ้ามี)



๕. ขอบเขตและข้อกำหนดความต้องการของระบบฯ ภายในโครงการ

๕.๑ ขอบเขตโครงการ (Project / System Scope)

๑) สำรวจจุดติดตั้งระบบรักษาความปลอดภัยและสำรวจระบบสารสนเทศที่จะดำเนินการทดสอบการเจาะระบบเพื่อหาช่องโหว่

๒) วิเคราะห์ระบบรักษาความปลอดภัยที่มีอยู่เดิม เพื่อดำเนินการเพิ่มประสิทธิภาพระบบ

๓) ออกแบบเพื่อติดตั้งระบบการรักษาความปลอดภัย

๔) ติดตั้งระบบรักษาความปลอดภัย และตรวจสอบระบบเพื่อหาช่องโหว่

๕) ทดสอบการทำงานของระบบ และทดสอบการใช้งานเครือข่ายและอินเตอร์เน็ต

๖) รายงานผลการทดสอบ

๗) ฝึกอบรมให้กับเจ้าหน้าที่ดูแลระบบ

๕.๒ ข้อกำหนดความต้องการของระบบ (System Requirements)

๑) มีระบบรักษาความปลอดภัยการถูกบุกรุกเว็บไซต์และระบบสารสนเทศอย่างมีประสิทธิภาพ

๒) มีระบบการวิเคราะห์และแจ้งเตือนภัยคุกคามได้โดยอัตโนมัติ และสามารถสร้างกฎ (Policy) โดยอัตโนมัติเพื่อป้องกันภัยคุกคามที่เกิดขึ้นได้อย่างทันเวลา

๓) สามารถตรวจสอบช่องโหว่ของเว็บไซต์และระบบสารสนเทศ เพื่อหาแนวทางและวิธีปิดช่องโหว่ที่เกิดขึ้น

๔) มีระบบป้องกันไวรัสที่มีประสิทธิภาพต่อการป้องกันไวรัส และมีลิขสิทธิ์ถูกต้องตามกฎหมาย

๖. แนวทางการดำเนินงาน รายการจัดหา ระยะเวลาดำเนินการ และกำหนดการ

๖.๑ แนวทางการดำเนินงาน

ดำเนินการจัดซื้อให้เป็นไปตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ ระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ กฎกระทรวงออกตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐

๖.๒ รายการที่จะจัดหา

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
๑. อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) **คุณลักษณะพื้นฐาน** - เป็นอุปกรณ์ Firewall ชนิด Next Generation Firewall แบบ Appliance - มี Firewall Throughput ไม่น้อยกว่า ๑๓๕ Gbps - รองรับ Threat Protection Throughput ๑๐ Gbps รองรับ Concurrent ได้ ๘ Million Sessions และรองรับการเชื่อมต่อใหม่ (New Sessions / Second) ได้ไม่น้อยกว่า ๕๕๐,๐๐๐ Sessions - สามารถทำการเชื่อมโยง IPsec VPN ซึ่งมีความเร็วในการทำงานไม่น้อยกว่า ๕๕ Gbps - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๑๖ ช่อง		✓	๒	๔,๓๔๐,๐๐๐	๘,๖๘๐,๐๐๐

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
- มีช่องสำหรับรองรับการเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑ Gbps (SFP) จำนวนไม่น้อยกว่า ๘ ช่อง และ ๑๐ Gbps (SFP+) จำนวนไม่น้อยกว่า ๔ ช่อง - สามารถตรวจสอบและป้องกันการบุกรุกรูปแบบต่างๆ อย่างน้อย ดังนี้ Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment เป็นต้นได้ - สามารถทำการกำหนด IP Address และ Service Port แบบ Network Address Translation (NAT) และ Port Address Translation (PAT) ได้ - สามารถทำงานลักษณะ Transparent Mode ได้ - สามารถ Routing แบบ Static, Dynamic Routing ได้ - มี Power Supply แบบ Redundant และ Hot Swap จำนวน ๒ หน่วย - สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย - สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้ - สามารถใช้งานตามมาตรฐาน IPv๖ ได้					
๒. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) **คุณลักษณะพื้นฐาน** - เป็นอุปกรณ์ทำหน้าที่ในการป้องกันด้าน Web Application หรือ Web Service โดยเฉพาะสามารถติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด ๑๙ นิ้ว ได้ - มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ ๑๐/๑๐๐/๑๐๐๐ Base-T หรือดีกว่า จำนวนไม่น้อยกว่า ๔ ช่อง และ ๑G SFP จำนวนไม่น้อยกว่า ๔ ช่อง - มีความเร็วในการส่งผ่านข้อมูล (Throughput) ไม่น้อยกว่า ๒.๕ Gbps หรือรองรับการส่งผ่านข้อมูลได้ไม่น้อยกว่า ๔๐,๐๐๐ Transactions ต่อวินาที - มีหน่วยเก็บข้อมูล Storage ขนาดไม่น้อยกว่า ๔๘๐ GB - สามารถบริหารจัดการอุปกรณ์ผ่านทางโปรแกรม Web Browser หรือ CLI ได้เป็นอย่างน้อย - สามารถตรวจจับพฤติกรรมการใช้งาน Web Application ของผู้ที่เข้ามาใช้บริการ Web Application บนเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ได้ - อุปกรณ์ที่นำเสนอจะต้องสามารถทำงานแบบ In-Line (Bridge) หรือ Transparent และ Span-mode (Monitor) สำหรับตรวจสอบพฤติกรรมได้เป็นอย่างน้อย		✓	๑	๕,๓๗๙,๕๐๐	๕,๓๗๙,๕๐๐

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
- มีความสามารถในการทำงานและปกป้อง Web Application ต่างๆ ได้ โดยรองรับ HTTPS ได้เป็นอย่างน้อย - สามารถเก็บและส่งรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) ในรูปแบบ Syslog ได้ - สามารถปรับเทียบเวลา (Time Synchronization) กับอุปกรณ์ภายนอกได้ - รองรับการป้องกันการถูกโจมตีด้วยวิธีต่างๆ ได้อย่างน้อย ดังนี้ - Cross-site Scripting - Cookie Poisoning - Buffer Overflow - SQL injection - สามารถทำรายงานการถูกโจมตีได้ในรูปแบบ HTML หรือ PDF หรือ XLS หรือดีกว่า - สามารถใช้งานตามมาตรฐาน IPv๖ ได้					
๓. ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM) **คุณลักษณะพื้นฐาน** - เป็นอุปกรณ์ประเภท Hardware Appliance ที่ออกแบบเฉพาะเพื่อทำหน้าที่เก็บบันทึกและวิเคราะห์ข้อมูลทางด้านการรักษาความปลอดภัยเครือข่าย (Security Information and Event Management) - สามารถรับ Log จากอุปกรณ์ได้อย่างน้อย ๑๐๐ อุปกรณ์ และวิเคราะห์ข้อมูลได้ไม่น้อยกว่า ๑,๕๐๐ เหตุการณ์ต่อวินาที (Events per Second) และรองรับการเพิ่มขยายได้สูงสุดไม่น้อยกว่า ๒๐,๐๐๐ เหตุการณ์ต่อวินาที (Events per Second) ได้ในอนาคต - มีพื้นที่ในการจัดเก็บข้อมูลไม่น้อยกว่า ๒๑ TB - สามารถเชื่อมโยงเหตุการณ์ต่าง ๆ เข้าด้วยกัน (Correlation) เพื่อตรวจจับรูปแบบเหตุการณ์ที่ซับซ้อนได้แบบ real time - สามารถเก็บ Log formats ในรูปแบบ Syslog ได้เป็นอย่างน้อย - สามารถแจ้งเตือนแบบ Real-time เมื่อมีเหตุการณ์ตรงตามเงื่อนไขที่สร้างไว้ และ เหตุการณ์ผิดปกติของตัวอุปกรณ์ผ่าน Email ได้เป็นอย่างน้อย - มี Threat Intelligences เพื่อรับข้อมูลภัยคุกคาม ได้ไม่น้อยกว่า Malware Domains, Malware IPs, Malware URLs		✓	๑	๖,๓๑๙,๓๐๐	๖,๓๑๙,๓๐๐

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	แบบ: ICT-MGNT๐๑-F๐๑
	** เข้าสู่การพิจารณาของคณะอนุกรรมการฯ ครั้งที่ ๑/๒๕๖๙	งบประมาณเกิน ๕ ล้านบาท

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
๔. ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection) **คุณลักษณะพื้นฐาน** - เป็นระบบที่ให้บริการในการป้องกันความเสี่ยงสินทรัพย์ดิจิทัล (Digital Risk Protection Service) ซึ่งการให้บริการในการตรวจสอบจะครอบคลุมบริเวณภายนอกองค์กรหรือเป็นส่วนที่ติดต่อกับโครงข่ายอินเทอร์เน็ต (Attack Surface) และพร้อมทั้งประเมินความเสี่ยงที่เกิดขึ้น - สามารถค้นหา (Discovered) รายละเอียดของสินทรัพย์ (Assets) ได้อย่างน้อย ได้แก่ IP Blocks IP Address และ Domain - สามารถทำแผนภาพความเชื่อมโยงระหว่างสินทรัพย์ในการค้นหาได้ - สามารถแสดงปริมาณความเสี่ยงที่เกิดขึ้น (Issues) ในระบบขององค์ได้ โดยสามารถอธิบายรายละเอียดของความเสี่ยงที่เกิดขึ้น พร้อมทั้งสามารถระบุสินทรัพย์ที่เข้าข่ายความเสี่ยงที่เกิดขึ้น (Affected assets) โดยสามารถจำแนกความเสี่ยงได้ - สามารถตรวจสอบการรั่วไหลของข้อมูลรหัสผู้ใช้งาน (Leaked Credentials) ในการเข้าใช้งานระบบขององค์กรได้ โดยสามารถสืบค้นทั้งจากแหล่งที่สามารถเข้าถึงได้ทั่วไป (Publicly Leaked) ซึ่งหากพบเจอข้อมูลรหัสผู้ใช้งานรั่วไหล ระบบสามารถระบุได้ว่าการรั่วไหลนั้นเกิดขึ้นจากเหตุการณ์ใด (Breach Name) พร้อมทั้งสามารถจำแนกได้ว่า มีองค์ประกอบของรหัสผ่านประกอบอยู่ด้วยหรือไม่ - สามารถทำงานร่วมกันกับระบบคลาวด์ต่างๆ เช่น AWS, Azure และ Google Cloud Platform (GCP) ได้เป็นอย่างน้อย - สามารถตรวจสอบระบบที่อยู่ภายในเครือค่ายได้ (Internal Attack Surface Management) โดยสามารถระบุความเสี่ยงของระบบ (internal vulnerability assessment) รวมถึงความเสี่ยงของเว็บแอพพลิเคชั่นได้ (web application analysis) ได้เป็นอย่างน้อย		✓	๑	๒,๓๔๐,๙๗๐	๒,๓๔๐,๙๗๐
๕. ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก **คุณลักษณะพื้นฐาน** - เป็นซอฟต์แวร์สำหรับติดตั้งบนเครื่องผู้ใช้ปลายทางเพื่อช่วยเพิ่มปลอดภัยบนเครื่องคอมพิวเตอร์สำหรับการยืนยันตัวตนเข้าสู่ระบบเครือข่าย - รองรับการพิสูจน์ตัวตน (Authentication) ร่วมกับ Local user, AD และ LDAP ได้เป็นอย่างน้อย หรือดีกว่า - สามารถติดตั้ง CA certificate เพื่อใช้กำหนด policy บนเครื่องผู้ใช้ปลายทางได้ - สามารถทำ SSL และ IPSec VPN และมีคุณสมบัติ auto-connect and always-up เพื่อความสะดวกในการใช้งาน		✓	๑๐๐	๖,๓๐๐	๖๓๐,๐๐๐

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
- สามารถทำ Two-Factor Authentication แบบ Mobile Token ได้ - ระบบบริหารจัดการจากส่วนกลาง (Centralized Management) ได้					
๖. ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response) **คุณลักษณะพื้นฐาน** - เป็นซอฟต์แวร์สำหรับช่วยป้องกัน และตอบสนองต่อเหตุการณ์แบบเรียลไทม์ โดยทำงานร่วมกับเวิร์กสเตชั่น และเซิร์ฟเวอร์ได้ - มีคุณสมบัติด้านความปลอดภัย ดังต่อไปนี้ - มี Virtual Patching หรือแสดงข้อมูลช่องโหว่บนเครื่องที่ติดตั้งได้เป็นอย่างน้อย - มี USB Control - สามารถป้องกันมัลแวร์ด้วย Machine-Learning ได้ - สามารถป้องกันอุปกรณ์ Endpoint ได้แม้จะอยู่ในสถานะออฟไลน์ - สามารถแสดงภาพกราฟตามลำดับขั้นตอนของเหตุการณ์ที่เกิดขึ้นได้เป็นอย่างน้อย - สามารถแสดงผลภัยคุกคามตาม MITRE attack framework - สามารถอัพเดต Threat Intelligence จากฐานข้อมูลของเจ้าของผลิตภัณฑ์ได้อย่างต่อเนื่องตลอดอายุสัญญา - สามารถทำการแจ้งเตือนผู้ดูแลระบบเมื่อพบมัลแวร์ผ่านทางระบบ Email และ Syslog ได้ - มีบริการ Managed Detection and Response Service (MDR) ที่ช่วยตรวจสอบ แจ้งเตือนภัยคุกคามและการจัดการเหตุการณ์ - มีระบบ eXtended Detection and Response (XDR) เพื่อช่วยตรวจสอบข้อมูลทางด้าน Security		✓	๑,๐๐๐	๘,๖๐๐	๘,๖๐๐,๐๐๐
๗. เครื่องคอมพิวเตอร์แม่ข่าย (Server) แบบ Hyper Converged Infrastructure (HCI) คุณลักษณะพื้นฐาน - มีหน่วยประมวลผลกลางไม่น้อยกว่า ๑๖ แกนหลัก (๑๖ core) และมีสัญญาณความเร็ว นาฬิกาไม่น้อยกว่า ๒.๙ GHz จำนวนไม่น้อยกว่า ๑ หน่วยต่อ Node Server - หน่วยความจำหลัก (RAM) ชนิด ECC DDR๔ หรือดีกว่า ความจุรวมไม่น้อยกว่า ๑๒๘ GB - มีช่องสำหรับติดตั้ง Hard Disk ได้จำนวนไม่น้อยกว่า ๘ หน่วย - มี Storage แบบ SSD ที่มีขนาดความจุ ไม่น้อยกว่า ๒๔๐ GB จำนวน ๑ หน่วย		✓	๓	๑,๕๕๐,๔๐๐	๔,๖๕๑,๒๐๐

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
- มี Storage แบบ SSD ที่มีขนาดความจุ ไม่น้อยกว่า ๙๖๐ GB จำนวน ๒ หน่วย - มี Storage แบบ SATA HDD ที่มีขนาดความจุ ไม่น้อยกว่า ๔ TB จำนวน ๒ หน่วย - มีหน่วยเชื่อมต่อระบบเครือข่ายแบบ ๑ Gigabit Ethernet จำนวนไม่น้อยกว่า ๔ พอร์ต - มี Remote Management Port (Out of band management) อย่างน้อย ๑ พอร์ต เพื่อช่วยในการจัดการกับ Server จากระยะไกลผ่าน Web Base Application (Remote) สามารถสั่ง Power ON, Power OFF, Restart เครื่อง Server - มี Power Supply แบบ Redundant ที่สามารถทำการถอดเปลี่ยนโดยไม่จำเป็นต้องหยุดระบบ หรือปิดเครื่อง (Hot-Swap) จำนวนไม่น้อยกว่า ๒ ชุด					
๘. ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย คุณลักษณะพื้นฐาน - สามารถทำ VM HA (High Availability) เพื่อให้ VM ทำงานได้อย่างต่อเนื่องในกรณีที่มี Node Down - สามารถย้าย VM ไปยัง Node อื่นได้ตามความเหมาะสมเพื่อรักษาประสิทธิภาพการทำงานของระบบได้โดยอัตโนมัติ เมื่อ Node ถูกใช้ CPU หรือ Memory มากเกินกว่าสัดส่วนที่กำหนดไว้ (Resource Scheduling) - สามารถเพิ่ม Resource ในส่วนของ CPU และ Memory ไปยัง VM แบบอัตโนมัติเมื่อ VM ถูกใช้ CPU หรือ Memory มากเกินกว่าสัดส่วนที่กำหนดไว้โดยไม่ต้องรีสตาร์ทหรือปิด VM ก่อน (Automated Hot Add) - สามารถเลือกทำสำเนาข้อมูลแบบ ๒ หรือ ๓ ในแต่ละ VM เพื่อลดความเสี่ยงไม่ให้เกิดการสูญหายของข้อมูลในกรณี Hard Disk ชำรุด - สามารถทำ Data Self-Balancing เมื่อมีการเพิ่ม Storage หรือ Node ได้ - สามารถทำงานแบบ SSD Caching, Storage Tiering และสามารถกำหนด Storage Policy (QoS) สำหรับ VM ได้ - มีความสามารถในการทำ Data-At-Rest Encryption หรือ Disk Encryption เพื่อช่วยรักษาความปลอดภัยของข้อมูล - มีความสามารถในการคำนวณพื้นที่การใช้งานของระบบล่วงหน้า Capacity หรือ Storage forecast ได้ - มีความสามารถหรือมีซอฟต์แวร์แสดง Real-Time Traffic Data เพื่อตรวจสอบปริมาณ Traffic ของ VM และ Distributed Switch ที่เกิดขึ้นในระบบ HCI ได้เป็นอย่างน้อย		✓	๑	๖,๒๕๐,๐๐๐	๖,๒๕๐,๐๐๐

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์	แบบ: ICT-MGNT๐๑-F๐๑
	** เข้าสู่การพิจารณาของคณะอนุกรรมการฯ ครั้งที่ ๑ /๒๕๖๘	งบประมาณเกิน ๕ ล้านบาท

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	Spec		จำนวน	ราคาต่อหน่วย	รวม
	DE	DEPT			
- มีความสามารถในการทำ Virtual Machine Snapshot ได้เป็นอย่างน้อย - มีความสามารถในการสำรองข้อมูลแบบ Scheduled Backup ได้แก่ Weekly, Daily และ Hourly โดยสามารถกำหนดระยะเวลาการเก็บรักษาข้อมูล (Retention Period) ได้					

* หมายเหตุ : ในรายการที่จัดหาให้ใช้เครื่องหมาย / ระบุใน SPEC ที่กำหนด
(DE:กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/ DEPT:หน่วยงานกำหนดเอง)

รายการ (อุปกรณ์ / ซอฟต์แวร์ / โปรแกรม / ระบบงาน)	จำนวน	ชื่อหน่วยงานที่ติดตั้ง
๑. อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)	๒	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)
๒. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	๑	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)
๓. ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM)	๑	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)
๔. ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection)	๑	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)
๕. ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก	๑	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)
๖. ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response)	๑	หน่วยงานส่วนกลางกรมป่าไม้
๗. เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า ๓ Node แบบ Hyper Converged Infrastructure (HCI)	๑	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)
๘. ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	๑	ห้องปฏิบัติการคอมพิวเตอร์ (Data Center)

๖.๔ ระยะเวลาดำเนินการ

ระยะเวลาดำเนินการ ๘ เดือน - ปี
เริ่มตั้งแต่ ตุลาคม ๒๕๖๘ ถึง พฤษภาคม ๒๕๖๙

๖.๕ กำหนดการ (Schedule)

กิจกรรม	กำหนดการ (เดือนที่)						หมายเหตุ
	๑	๒	๓	๔	๕	๖	
๑. สำรวจจุดติดตั้งระบบรักษาความปลอดภัยและสำรวจระบบสารสนเทศที่จะดำเนินการทดสอบการเจาะระบบเพื่อหาช่องโหว่	←	→					
๒.วิเคราะห์ระบบรักษาความปลอดภัยที่มีอยู่เดิม เพื่อดำเนินการเพิ่มประสิทธิภาพระบบ		←	→				
๓.ออกแบบเพื่อติดตั้งระบบการรักษาความปลอดภัย			←	→			

ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์

** เข้าสู่การพิจารณาของคณะอนุกรรมการฯ ครั้งที่ ๑/๒๕๖๑

แบบ: ICT-MGNT๐๑-F๐๑

งบประมาณเกิน ๕ ล้านบาท

กิจกรรม	กำหนดการ (เดือนที่)						หมายเหตุ
	๑	๒	๓	๔	๕	๖	
๔. ติดตั้งระบบรักษาความปลอดภัยและทดสอบการเจาะระบบเพื่อหาช่องโหว่				←→	←→		
๕. ทดสอบการทำงานของระบบรักษาความปลอดภัย และทดสอบการใช้งานเครือข่ายและอินเตอร์เน็ต					←→		
๖. รายงานผลการทดสอบ						←→	
๗. ฝึกอบรมให้กับเจ้าหน้าที่ดูแลระบบ						←→	
๘. ส่งมอบงาน						←→	

๗. ผลผลิตของโครงการ (Output / Deliverables)

ได้อุปกรณ์และซอฟต์แวร์ที่มีประสิทธิภาพต่อการป้องกันไวรัส WannaCry ransomware ไวรัส Botnet และป้องกันการถูกเจาะระบบสารสนเทศและฐานข้อมูลของกรมป่าไม้

๘. ตัวชี้วัดสัมฤทธิ์ผล หรือปัจจัยสำเร็จของโครงการ

ได้รับการสนับสนุนจากผู้บริหารกรมป่าไม้และได้รับการจัดสรรงบประมาณในการดำเนินการ

๙. ความสอดคล้องเชิงยุทธศาสตร์ของโครงการ

๙.๑ ความสอดคล้องกับแผนยุทธศาสตร์ชาติ / แผนการปฏิรูปประเทศ / แผนปฏิบัติราชการของหน่วยงาน

๑) ยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๑ – ๒๕๘๐ ด้านการสร้างความสามารถในการแข่งขัน พัฒนาโครงสร้างพื้นฐานเทคโนโลยีสมัยใหม่

๒) ยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๑ – ๒๕๘๐ ด้านการสร้างความสามารถในการแข่งขัน สร้างโอกาสเข้าถึงข้อมูล

๙.๒ ความสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม / แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคม

๑) แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๓

หมุดหมายที่ ๖ ไทยเป็นฐานการผลิตอุปกรณ์อิเล็กทรอนิกส์อัจฉริยะที่สำคัญของโลก

กลยุทธ์ที่ ๔ พัฒนาระบบนิเวศเพื่อสนับสนุนการพัฒนาอุตสาหกรรมอิเล็กทรอนิกส์อัจฉริยะ อุตสาหกรรม และบริการดิจิทัล

กลยุทธ์ย่อยที่ ๔.๑ พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีที่มีคุณภาพ ครอบคลุม เพียงพอและเข้าถึง ได้ ทั้งในด้านพื้นที่และราคา เพื่อให้ประชาชนมีความคุ้มครองทางสังคมที่เพียงพอ เหมาะสม สามารถเข้าถึง การศึกษา สาธารณสุข บริการภาครัฐ และโอกาสทางเศรษฐกิจและสังคมอื่น ๆ รวมทั้งรองรับกับปริมาณความ ต้องการใช้งานทางดิจิทัลในอนาคต ทั้งในเชิงคุณภาพและเชิงปริมาณ

๒) แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. ๒๕๖๖-๒๕๗๐

ยุทธศาสตร์ที่ ๑ ยกระดับคุณภาพการให้บริการแก่ประชาชนด้วยเทคโนโลยีดิจิทัล

มาตรการ ๔) เพิ่มความสามารถ ความมั่นคงปลอดภัยในการประยุกต์ใช้เทคโนโลยีดิจิทัลภาครัฐพร้อมทั้งจัดหากลไกการป้องกันคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการรับบริการจากภาครัฐ (แผนที่ ๖,๗

๙.๓ แผนของกระทรวงหรือแผนของหน่วยงาน

๙.๓.๑ ความสอดคล้องกับแผนยุทธศาสตร์ชาติกรมป่าไม้ระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ – ๒๕๗๙)

๑) ยุทธศาสตร์ที่ ๖ บูรณาการและส่งเสริมการมีส่วนร่วมทุกภาคส่วน

๒) ยุทธศาสตร์ที่ ๗ การพัฒนาระบบบริหารและจัดการองค์กร

๙. ความสอดคล้องเชิงยุทธศาสตร์ของโครงการ

๙.๓.๒ สอดคล้องกับแผนปฏิบัติการดิจิทัลของกรมป่าไม้ (พ.ศ. ๒๕๖๕-๒๕๖๘)

-

๙.๔ พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑๐. ความพร้อมของโครงการ

๑๐.๑ บุคลากรของหน่วยงานที่เกี่ยวข้องกับโครงการ (ตามข้อ ๑.)

ด้าน / สาขา	จำนวน
ข้าราชการ กรมป่าไม้	๑,๖๙๖
ลูกจ้างประจำ กรมป่าไม้	๖๒๙
พนักงานราชการ กรมป่าไม้	๖,๖๐๐
รวม	๘,๙๒๕

๑๐.๒ ประเด็นความพร้อมด้านอื่นๆ (ถ้ามี)

มีเจ้าหน้าที่ด้านเทคนิคที่มีความรู้ความสามารถในการติดตั้งและดูแลเครือข่าย และมีที่ปรึกษาในการวิเคราะห์ ออกแบบระบบการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพ

๑๐.๓ ประเด็นความเสี่ยงของโครงการและแนวทางการบรรเทา (Project Risks and Risk Mitigations)

-

๑๑. ประโยชน์ที่จะได้รับ

๑. สามารถป้องกันการโจมตี การเจาะระบบสารสนเทศและระบบเครือข่ายของกรมป่าไม้
๒. สามารถค้นหา วิเคราะห์ แสดงผล และแจ้งเตือนภัยคุกคามที่เกิดขึ้นได้โดยอัตโนมัติ
๓. สามารถปิดช่องโหว่ที่เกิดขึ้นในระบบสารสนเทศและระบบเครือข่าย
๔. สามารถปฏิบัติตามข้อกำหนดตามหลักเกณฑ์ของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในหมวดหมู่ของการป้องกันได้อย่างมีประสิทธิภาพ

	ข้อเสนอโครงการจัดหาระบบคอมพิวเตอร์ ** เข้าสู่การพิจารณาของคณะอนุกรรมการฯ ครั้งที่ ๑/๒๕๖๘	หน้า ๑๔ /๑๔ แบบ: ICT-MGNT๐๑-F๐๑ งบประมาณเกิน ๕ ล้านบาท

ค. การลงนามรับรองโครงการ

๑. ผู้จัดทำ / ขออนุมัติโครงการ

ลงชื่อ.....

(นายทนงศักดิ์ มนตรี)

ตำแหน่ง นักวิชาการคอมพิวเตอร์ชำนาญการ

หน่วยงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้

๒. ผู้ตรวจสอบโครงการ

ลงชื่อ.....

(นายสัมพันธ์ มีสิทธิ์)

ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

หน่วยงาน กรมป่าไม้

๓. ผู้รับผิดชอบโครงการระดับกรม / รัฐวิสาหกิจ

ลงชื่อ.....

(นายนิกร ศิรโรจนานนท์)

ตำแหน่ง รองอธิบดีกรมป่าไม้

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)

ของกรมป่าไม้

๔. ผู้รับรองผลการพิจารณาอนุมัติโครงการจากคณะกรรมการบริหารเทคโนโลยีสารสนเทศระดับสูงและกำกับดูแลธรรมาภิบาลข้อมูลของกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

โครงการฯ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริหารเทคโนโลยีสารสนเทศระดับสูงและกำกับดูแลธรรมาภิบาลข้อมูลของกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เมื่อวันที่ 10 กพ. 2568

ลงชื่อ.....

(นายสิทธิชัย เสรีส่งแสง)

ตำแหน่ง รองปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (MCIO)

ของกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม

MCS Asia Limited.

บริษัทไอเอ็มซีเอส เอเชีย จำกัด

Quotation
ใบเสนอราคา

บริษัทไอเอ็มซีเอส เอเชีย จำกัด
168/105 หมู่1 ถ.345 ต.บางขะแยง อ.เมืองปทุมธานี
จ.ปทุมธานี 12000
Tel: +66 (0)20597255, Fax: +66 (0)20597255
Website: http://www.imcs.asia
เลขประจำตัวผู้เสียภาษี: 0105554121615 (สำนักงานใหญ่)

Quotation No. Q202411-025

ชื่อลูกค้า/Client Name : กรมป่าไม้
เลขประจำตัวผู้เสียภาษี:

Date: 18-Nov-24

Quoted by:

ที่อยู่/Address:

Donlathan Wiwat

โทร/Tel:
Fax:
Attention:

Tel: +66 62 782 4526

Project โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

We are pleased to respond

Item	Product	Description	Qty	Unit	Price	Total Amount
		โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้				
1		อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) Paloalto PA-5450	2		8,558,000.00	17,116,000.00
2		อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) Imperva X8530	1		6,350,000.00	6,350,000.00
3		ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM) IBM QRadar	1		6,890,000.00	6,890,000.00
4		ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection) Mandiant	1		3,567,900.00	3,567,900.00
5		ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก Paloalto Prisma Access	100		9,900.00	990,000.00
6		ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response) Paloalto Cortex XDR for Endpoint	1000		12,000.00	12,000.00
7	HPE-DL380	เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า 3 Node แบบ Hyper Converged Infrastructure (HCI) HPE ProLiant DL380 Gen10 Plus Server	1		4,970,000.00	4,970,000.00
8		ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย Vmware Standard	1		8,790,000.00	8,790,000.00
		Total				**48,685,900.00**
		VAT 7%				**Include**
		Sub Amount				**48,685,900.00**

Total Amount (in words) : (สี่สิบแปดล้านหกแสนแปดหมื่นห้าพันเก้าร้อยบาทถ้วน)

Donlathan W. **Authorized Signature** **(Mr. Donlathan Wiwat)** **Project Manager**	**Commerical terms & conditions:** **Price Validity : 120 Days** **Delivery Time : 30 Days** **Credit Term :** The above prices are valid for whole lists of this quotation and must be placed in one PO. We reserve the right to change the stock status without notice

บริษัท ไอเอ็มซีเอส เอเชีย จำกัด

MILLENNIUM PLUS NETWORK CO.,LTD.
1178/204 Soi Phahonyothin 32 , Chankasem,Chatuchak, Bangkok, 10900
(Head Office) Tel. 02-561-2119

Quotation

No: AS202411043
Date: 18-Nov-2024

Company: กรมป่าไม้
Attn:
Address:
Tel :
E-mail:

Project : โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัย
Refer Code : ไซเบอร์ กรมป่าไม้
Contact : Mr. Anucha
Tel : 02-561-2119, 080-936-2597
E-mail : Anucha@millenniumplus.co.th

We are pleased to submit you the following quotation and offer to sell the product descriped herein at price, items, and terms stated

Item	Part Number	Description	Qty.	Unit Price (Baht)	Item Total (Baht)
		โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้			
1	อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)	Cisco Secure Firewall 4245	2	8,697,000.00	17,394,000.00
2	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	F5 i4800	1	6,890,000.00	6,890,000.00
3	ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM)	Cisco Splunk	1	9,800,000.00	9,800,000.00
4	ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection)	Group IB	1	4,506,000.00	4,506,000.00
5	ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก	Cisco Secure client	100	10,000.00	1,000,000.00
6	ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response)	Sentinel One	1,000	15,900.00	15,900,000.00
7	เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า 3 Node แบบ Hyper Converged Infrastructure (HCI) Lenovo HX5531	Lenovo ThinkAgile HX5531-G	1	5,016,000.00	5,016,000.00
8	ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย Vmware	vSphere Foundation	1	9,704,000.00	9,704,000.00
		เจ็ดสิบล้านสองแสนหนึ่งหมื่นบาทถ้วน		**Total**	70,210,000.00
				Vat7%	Include
				Grand Total	70,210,000.00

Terms & Conditions :

1	Price Validity	120 Days
2	Terms of Payment	
3	Delivery	
4	Warranty Period	

Please confirm your acceptance of this quote by signing this document

Authorized Signature:

.....

(.....)

Prepared By:

.....

Mr. Anucha Sangsuriyan
Sales Executive / Tel.080 936 2597

TPS
The Practical Solution
Public Company Limited

+66 2112 9999
+66 2112 9998
thepractical
www.thepractical.co.th
99 Soi Cement Thai, Ratchadapisek Road,
Lad Yao, Chatuchak, Bangkok 10900 Thailand
TAX ID: 0-1075-62000-30-1

QUOTATION

COMPANY : กรมป่าไม้
ADDRESS :

ATTENTION : นายทนงศักดิ์ มนตรี
E-MAIL :
TEL :
FAX :

QUOTATION NO. : TPS-AMT2411-026 **Rev.0**
DATE : November 18, 2024

QUOTE / PRICE DESCRIPTION : โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

ITEM	PART NUMBER	DESCRIPTION	QUANTITY	UNIT PRICE (BAHT)	ITEM TOTAL (BAHT)
โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้					
		1. อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)	2	4,340,000.00	8,680,000.00
		FortiGate-600F			
		2. อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	1	5,379,500.00	5,379,500.00
		FortiWeb-1000F			
		3. ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM)	1	6,319,300.00	6,319,300.00
		FortiSIEM-2200G			
		4. ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection)	1	2,340,000.00	2,340,000.00
		FortiRecon			
		5. ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก	100	6,300.00	630,000.00
		FortiTokenMobile			
		6. ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response)	1000	8,550.00	8,550,000.00
		FortiEDR-XDR			
		7. เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า 3 Node แบบ Hyper Converged Infrastructure (HCI)	1	4,651,200.00	4,651,200.00
		NX-1365N-G8			
		8. ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	1	6,250,000.00	6,250,000.00
		Software Nutanix			

Authorized Signature / ลงนามอนุมัติการสั่งซื้อ

(_____)

_____/_____/_____

REMARK :		
	TOTAL	42,800,000.00
	VAT 7%	Inc.
	GRAND TOTAL	42,800,000.00

TERMS & CONDITIONS

1. Price Validity 120 Days
2. Delivery
3. Terms of Payment
4. Warranty Period 1 Year
5. Please send us your purchase order or simply sign above to confirm the ordering using e-mail: **order@thepractical.co.th** or fax number: **+66 2 112 9998**

PREPARED BY

(Monticha Thanasaro)
Account Manager
Mobile: 090-695-5633
Email: Monticha@thepractical.co.th

MCS Asia Limited.

บริษัทไอเอ็มซีเอส เอเชีย จำกัด

บริษัทไอเอ็มซีเอส เอเชีย จำกัด
168/105 หมู่1 ถ.345 ต.บางขะแยง อ.เมืองปทุมธานี
จ.ปทุมธานี 12000
Tel: +66 (0)20597255, Fax: +66 (0)20597255
Website: http://www.imcs.asia
เลขประจำตัวผู้เสียภาษี: 0105554121615 (สำนักงานใหญ่)

Quotation
ใบเสนอราคา

Quotation No. Q202411-025

Date: 18-Nov-24

Quoted by:

Donlathan Wiwat

Tel: +66 62 782 4526

ชื่อลูกค้า/Client Name : กรมป่าไม้
เลขประจำตัวผู้เสียภาษี:

ที่อยู่/Address:

โทร/Tel:
Fax:
Attention:
Project โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

We are pleased to respond

Item	Product	Description	Qty	Unit	Price	Total Amount
		โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้				
1	อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)	Paloalto PA-5450	2		8,558,000.00	17,116,000.00
2	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)	Imperva X8530	1		6,350,000.00	6,350,000.00
3	ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM)	IBM QRadar	1		6,890,000.00	6,890,000.00
4	ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection)	Mandiant	1		3,567,900.00	3,567,900.00
5	ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก	Paloalto Prisma Access	100		9,900.00	990,000.00
6	ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response)	Paloalto Cortex XDR for Endpoint	1000		12,000.00	12,000.00
7	เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า 3 Node แบบ Hyper Converged Infrastructure (HCI)	HPE ProLiant DL380 Gen10 Plus Server	1		4,970,000.00	4,970,000.00
	HPE-DL380					
8	ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	Vmware Standard	1		8,790,000.00	8,790,000.00
		Total				**48,685,900.00**
		VAT 7%				**Include**
		Sub Amount				**48,685,900.00**

Total Amount (in words) : (สี่สิบแปดล้านหกแสนแปดหมื่นห้าพันเก้าร้อยบาทถ้วน)

Donlathan W. **Authorized Signature** **(Mr. Donlathan Wiwat)** **Project Manager**	**Commerical terms & conditions:** **Price Validity : 120 Days** **Delivery Time : 30 Days** **Credit Term :** The above prices are valid for whole lists of this quotation and must be placed in one PO. We reserve the right to change the stock status without notice

บริษัท ไอเอ็มซีเอส เอเชีย จำกัด

MILLENNIUM PLUS NETWORK CO.,LTD.
1178/204 Soi Phahonyothin 32 , Chankasem,Chatuchak,
Bangkok, 10900
(Head Office) Tel. 02-561-2119

Quotation

No: AS202411043
Date: 18-Nov-2024

Company: กรมป่าไม้
Attn:
Address:
Tel :
E-mail:

Project : โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัย
Refer Code : ไซเบอร์ กรมป่าไม้
Contact : Mr. Anucha
Tel : 02-561-2119, 080-936-2597
E-mail : Anucha@millenniumplus.co.th

We are pleased to submit you the following quotation and offer to sell the product descriped herein at price, items, and terms stated

Item	Part Number	Description	Qty.	Unit Price (Baht)	Item Total (Baht)
		โครงการเพิ่มประสิทธิภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้			
1	อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall)		2	8,697,000.00	17,394,000.00
		Cisco Secure Firewall 4245			
2	อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)		1	6,890,000.00	6,890,000.00
		F5 i4800			
3	ระบบวิเคราะห์ภัยคุกคามบนเครือข่าย (Security Incident Event Management: SIEM)		1	9,800,000.00	9,800,000.00
		Cisco Splunk			
4	ระบบการป้องกันความเสี่ยงดิจิทัล (Digital Risk Protection)		1	4,506,000.00	4,506,000.00
		Group IB			
5	ซอฟต์แวร์ยืนยันตัวตนการเชื่อมต่อเครือข่ายจากภายนอก		100	10,000.00	1,000,000.00
		Cisco Secure client			
6	ชุดโปรแกรมป้องกันไวรัส (Endpoint Detection and Response)		1,000	15,900.00	15,900,000.00
		Sentinel One			
7	เครื่องคอมพิวเตอร์แม่ข่าย (Server) จำนวนไม่น้อยกว่า 3 Node แบบ Hyper Converged Infrastructure (HCI)		1	5,016,000.00	5,016,000.00
	Lenovo HX5531	Lenovo ThinkAgile HX5531-G			
8	ชุดโปรแกรมระบบคอมพิวเตอร์เสมือนสำหรับเครื่องคอมพิวเตอร์แม่ข่าย		1	9,704,000.00	9,704,000.00
	Vmware	vSphere Foundation			
		เจ็ดสิบล้านสองแสนหนึ่งหมื่นบาทถ้วน		**Total**	70,210,000.00
				Vat7%	Include
				Grand Total	70,210,000.00

Terms & Conditions :

1	Price Validity	120 Days
2	Terms of Payment	
3	Delivery	
4	Warranty Period	

Please confirm your acceptance of this quote by signing this document

Authorized Signature:

.....

(.....)

Prepared By:

.....

Mr. Anucha Sangsuriyan
Sales Executive / Tel.080 936 2597