เอกสารนำเสนอ

คณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์

ของกรมการปกครอง

โครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) ตาม พ.ร.บ. รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ประจำปีงบประมาณ พ.ศ. 2568

งบประมาณ 2,135,000 บาท

หน่วยงาน ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง

มกราคม 2567

สารบัญ

ภาคผนวก ก.

แบบรายงานสรุปโครงการเพื่อพิจารณาความเหมาะสมของคุณลักษณะเฉพาะและราคา (ก่อนการจัดหา)

☐ เสนอคณะกรรมการฯ ของ มท. เพื่อพิจารณาให้ความเห็นชอบในหลักการ

√ เสนอคณะกรรมการฯ ของ ปค. เพื่อพิจารณาให้ความเห็นชอบในหลักการ (ได้รับความเห็นชอบในหลักการจากคณะกรรมการฯ ของ ปค. ในการประชุมครั้งที่ ..... เมื่อวันที่ .....)

ชื่อ โครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) ประจำปีงบประมาณ พ.ศ. 2568

รวมวงเงินโครงการ จำนวนเงิน 2,284,450 บาท

ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์ จำนวนเงิน 2,284,450 บาท

ชื่อหน่วยงาน ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง

ส่วนที่เป็นอุปกรณ์คอมพิวเตอร์

กรณีตรงตามเกณฑ์ของกระทรวงดิจิทัลฯ หรือเกณฑ์ที่ส่วนราชการอื่นประกาศกำหนด

ลำดับ	รายการ	ข้อ (ตามเกณฑ์ MICT)	ราคา MICT	ราคาอ้างอิง	จำนวน	วงเงินรวม

กรณีไม่มีราคาตามเกณฑ์ของกระทรวงดิจิทัลฯ หรือเกณฑ์ที่ส่วนราชการอื่นประกาศกำหนด

ลำดับ	รายการ	การสืบราคาจากท้องตลาด รวมทั้งเว็บไซต์ต่างๆ (เปรียบเทียบอย่างน้อย ๓ ราย/ ๓ ยี่ห้อ รวมทั้งเว็บไซต์อย่างน้อย ๑ เว็บไซต์)				ราคาอ้างอิง	จำนวน	วงเงินรวม	หมายเหตุ
		SO BE IT (โซ บี อิท โซลูชั่น)	Point IT Consulting Co.,Ltd.	KT Professional (เค ที โปรเฟสชั่นแนล)	รวมทั้งเว็บไซต์ (อย่างน้อย ๑ เว็บไซต์)				
1	ระบบตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing)	2,284,450.00	2,578,700.00	2,418,200.00		2,284,450.00	1	2,284,450.00	
	รวมจำนวนเงินที่ไม่เป็นไปตามเกณฑ์ราคากลางฯ							2,284,450.00	

ส่วนที่เป็นอุปกรณ์อื่นๆ

ลำดับ	รายการ	จำนวนเงิน	จำนวน	จำนวนเงินรวม
			ภาษีมูลค่าเพิ่ม ๗%	
			รวมงบประมาณทั้งโครงการ	2,284,450

หมายเหตุ

๑. การสืบราคาจะต้องสืบทั้งจากท้องตลาดรวมทั้งเว็บไซต์ หากมีใช้ราคาต่ำสุดเป็นราคาอ้างอิง ให้ระบุเหตุผลประกอบด้วย

๒. สำหรับการพัฒนาซอฟต์แวร์ประเภทโปรแกรมประยุกต์ให้จัดทำรายละเอียดตามแบบบัญชีราคากลางพัฒนาระบบประเภทโปรแกรมประยุกต์ที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนด

๓. ราคาตามเกณฑ์ราคากลางและคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นราคาที่รวมภาษีมูลค่าเพิ่มแล้ว ๗% กรณีไม่มีราคาตามเกณฑ์ฯ

ส่วนที่ 1 บทสรุปโครงการ

1. ชื่อโครงการและหน่วยงานที่รับผิดชอบ

ชื่อโครงการ : โครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing)) ตาม พ.ร.บ. รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประจำปีงบประมาณ พ.ศ. 2568

หน่วยงานที่รับผิดชอบ : ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง กระทรวงมหาดไทย

2. วัตถุประสงค์และเป้าหมายของโครงการ

2.1 วัตถุประสงค์

1) เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามด้านไซเบอร์และเตรียมความพร้อมในการรับมือกับภัยคุกคามทั้งภายในและภานนอก
2) เพื่อวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศทำการทดสอบการเจาะหาช่องโหว่ เครือข่ายจากภายในและภายนอกพร้อมทั้งรับข้อเสนอแนะในการปรับปรุงระบบความปลอดภัยที่เกี่ยวข้อง
3) เพื่อเพิ่มความปลอดภัย และเพิ่มการป้องกันจากการโจมตีของผู้ไม่ประสงค์ดี
4) สร้างความหน้าเชื่อถือและเพิ่มความมั่นใจในการใช้งาน

2.2 เป้าหมาย

จัดหาระบบตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) 1 ระบบ สำหรับการประเมินความมั่นคงปลอดภัยของระบบสารสนเทศภายในหน่วยงานเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยผู้ตรวจสอบภายในหน่วยงานของ ปค. (โปรแกรมทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่ในระบบ network)

3. ขอบเขตการดำเนินโครงการกับหน้าที่ความรับผิดชอบ

3.1 ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง มีอำนาจหน้าที่

ศสป. เป็นหน่วยงานที่มีภารกิจหลักในการพัฒนาและปรับปรุงระบบสารสนเทศของ ปค. เพื่อสนับสนุนนโยบายที่ ปค. ได้รับมอบหมายจากรัฐบาล มท. และ ของ ปค. ให้ดำเนินงานตามนโยบายและภารกิจสำคัญได้อย่างมีประสิทธิภาพ เสนอแนะนโยบายและจัดทำแผนแม่บทกลยุทธ์ และแผนปฏิบัติการเทคโนโลยีสารสนเทศ รวมทั้งกำกับ ติดตาม และประเมินผล บริหารและพัฒนาระบบสารสนเทศ ศึกษาวิเคราะห์ ออกแบบ และประยุกต์ใช้นวัตกรรมระบบสารสนเทศเพื่อพัฒนาการบริหารงานของศูนย์ปฏิบัติการกรม และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศเพื่อการบริหารราชการระดับอำเภอ พัฒนาบุคลากรและจัดทำหลักสูตรฝึกอบรมด้านการใช้เทคโนโลยีสารสนเทศ ตลอดจนปฏิบัติงานเลขานุการ

คณะกรรมการข้อมูลสารสนเทศกรมการปกครอง และงานอื่น ๆ ที่ได้รับมอบหมาย แบ่งโครงสร้างภายในออกเป็น 1 ฝ่าย 4 กลุ่มงาน ได้แก่

1) ฝ่ายบริหารงานทั่วไป

2) กลุ่มงานวิเคราะห์และพัฒนา

3) กลุ่มงานปฏิบัติการและประมวลผลข้อมูล

4) กลุ่มงานพัฒนาการเรียนรู้และบูรณาการระบบสารสนเทศ

5) กลุ่มงานขับเคลื่อนการบริหารงานปกครองแบบดิจิทัล

3.2 ขั้นตอนการดำเนินงาน

จัดทำคำของบประมาณในปี ๒๕๖๘ เมื่อได้รับการอนุมัติงบประมาณ ดำเนินการโดยวิธี e-bidding

๓.๓ กลุ่มเป้าหมาย/ผู้ได้รับผลประโยชน์

ผู้ใช้ระบบสารสนเทศของกรมการปกครอง

๔. ระบบงานที่จะดำเนินในโครงการ

๔.๑ ปัญหาและอุปสรรคในการปฏิบัติงานและความจำเป็นที่ต้องจัดทำโครงการ

กรมการปกครองโดยศูนย์สารสนเทศเพื่อการบริหารงานปกครอง ได้มีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยในการปฏิบัติงานต่างๆ มากขึ้นทั้งในส่วนของสายงานหลัก และสายงานสนับสนุน รวมทั้งใช้เป็นช่องทางหนึ่งในการเผยแพร่ข้อมูลข่าวสารต่างๆ มีการเชื่อมต่อเครือข่ายภายในกับเครือข่ายภายนอกทำให้มีความเสี่ยงจากภัยคุกคามในรูปแบบต่างๆ ที่มีต่อระบบสารสนเทศขององค์กรและเกิดภัยคุกคามทางไซเบอร์ จำเป็นต้องมีความพร้อมในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์หลายด้าน อาทิ งานโครงสร้างพื้นฐาน การเฝ้าระวัง ป้องกันและแก้ปัญหา การตรวจสอบช่องโหว่ของระบบสารสนเทศ รวมถึงเว็บไซต์ซึ่งมักจะเป็นเป้าถูกโจมตีอยู่บ่อยครั้ง นอกจากนี้ จึงจำเป็นต้องเสริมสร้างขีดความสามารถในการรับมือกับไซเบอร์ขององค์กร

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ดังนั้นเพื่อให้แน่ใจว่าการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กรมีความเพียงพอ และมีประสิทธิผล จึงมีความจำเป็นต้องเสริมสร้างขีดความสามารถในการรับมือกับไซเบอร์ขององค์กรให้มีประสิทธิภาพยิ่งขึ้นกว่าเดิม โดยจัดทำโครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) ประจำปีงบประมาณ พ.ศ. 2568 ขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมการปกครองเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ อีกทั้งในปัจจุบันยังไม่มีการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้วยวิธีการทดสอบเจาะหาช่องโหว่ให้

มั่นใจว่าระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรมีระบบการป้องกันที่รัดกุมเพียงพอ และสามารถป้องกันการโจมตีผ่านช่องทางต่างๆ ทุกรูปแบบ และเป็นการดำเนินการตามพ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และแผนยุทธศาสตร์ชาติ 20 ปี

4.2 ระบบงานที่ขออนุมัติ

โปรแกรมการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) จำนวน 1 ระบบ โดยมี license พร้อมการรับประกัน 12 เดือน

5. การเตรียมบุคลากรผู้ปฏิบัติโครงการ

การดำเนินโครงการจะใช้บุคลากรที่มีตำแหน่งงานและความรู้ด้านคอมพิวเตอร์ ซึ่งมีอยู่เดิม 10 คน และมีแผนเพิ่มบุคลากรที่เกี่ยวข้อง เพื่อเพิ่มประสิทธิภาพความเข้มแข็งของระบบงานให้สำเร็จได้ตามเป้าหมาย รวมทั้งจัดให้มีการฝึกอบรมด้านคอมพิวเตอร์ให้กับผู้ปฏิบัติงานและผู้บริหารระดับต่าง ๆ ให้มีความรู้สามารถทำงานได้ดังนี้

5.1 สามารถวิเคราะห์กำหนดคุณลักษณะของเครื่อง จัดระบบติดตั้งเชื่อมโยงระบบเครื่องคอมพิวเตอร์ ศึกษาวิเคราะห์ออกแบบเกี่ยวกับชุดคำสั่งระบบ ชุดคำสั่งประยุกต์ รวมทั้งการเขียนคู่มืออธิบายการใช้คำสั่งต่าง ๆ ให้คำปรึกษาแนะนำการอบรมเกี่ยวกับวิทยาการคอมพิวเตอร์ด้านต่าง ๆ แก่บุคลากรหรือหน่วยงาน ติดตามความก้าวหน้าของเทคโนโลยีสมัยใหม่

5.2 สามารถควบคุม ดูแล ซ่อมแซม ตรวจสอบการทำงาน แก้ไขปัญหาการใช้งานของระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบเครือข่ายสื่อสาร รวมทั้งระบบสนับสนุนต่าง ๆ เพื่อให้ระบบงานสามารถทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ

6. วงเงินค่าใช้จ่าย

ใช้งบประมาณรายจ่าย ประจำปีงบประมาณ พ.ศ. 2568 แผนงาน : ยุทธศาสตร์พัฒนาบริการประชาชนและการพัฒนาประสิทธิภาพภาครัฐ ผลผลิต : โครงการสนับสนุนการบูรณาการงานในพื้นที่เพื่อพัฒนาประสิทธิภาพภาครัฐ กิจกรรมหลัก : สนับสนุนการปฏิบัติงานของอำเภอ โครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) ประจำปีงบประมาณ พ.ศ. 2568 งบลงทุน หมวดค่าครุภัณฑ์คอมพิวเตอร์สูงกว่า 1 ล้านบาท จำนวน 2,284,450 บาท

ส่วนที่ 2 รายละเอียดโครงการที่เสนอขออนุมัติ

1. ชื่อโครงการ

1.1 ชื่อโครงการ : โครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing)) ตาม พ.ร.บ. รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประจำปีงบประมาณ พ.ศ. 2568

1.2 ความสอดคล้องกับยุทธศาสตร์ระดับชาติ

1.2.1 ยุทธศาสตร์ชาติระยะ 20 ปี (พ.ศ. 2561 – พ.ศ. 2580) ด้านที่ 1 ด้านความมั่นคง การพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลในภาพรวมของกรมการปกครอง และด้านที่ 6 ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ ประเด็นยุทธศาสตร์ที่ 1 ภาครัฐที่ยึดประชาชนเป็นศูนย์กลางตอบสนองความต้องการ และให้บริการอย่างสะดวกรวดเร็ว

1.2.2 แผนแม่บทภายใต้ยุทธศาสตร์ (พ.ศ. 2561 – 2580) การวิจัยและพัฒนานวัตกรรม ด้านสังคม ปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ โดยการส่งเสริมการวิจัย พัฒนา และประยุกต์ใช้นวัตกรรมในการพัฒนาการบริหารจัดการภาครัฐ เพื่อให้มีความทันสมัย ตอบสนองความต้องการและให้บริการประชาชนได้อย่างสะดวกรวดเร็ว และโปร่งใส

1.2.3 แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑3 มิติที่ 4 หมุดหมายที่ 13 ไทยมีภาครัฐที่ทันสมัย มีประสิทธิภาพและตอบโจทย์ประชาชน ภาครัฐเป็นกลไกหลักในการดูแลประชาชนให้กินดีอยู่ดี และเคลื่อนการพัฒนาประเทศ โดยมีหน้าที่และบทบาทสำคัญในการให้บริการประชาชน กลยุทธ์ที่ 3 การปรับเปลี่ยนภาครัฐเป็นรัฐบาลดิจิทัลที่ใช้ข้อมูลในการบริหารจัดการเพื่อการพัฒนาประเทศ

1.2.4 แผนการปฏิรูปประเทศ ด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ การปฏิรูประบบการบริหารจัดการข้อมูลข่าวสารภาครัฐ

1.2.5 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ การเสริมสร้างความมั่นคงของมนุษย์

1.2.6 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 การขับเคลื่อนให้เกิดการปฏิรูปการบริหารราชการแผ่นดินและการบริการประชาชน โดยมีระบบการทำงานแบบบูรณาการและมีการเชื่อมโยงข้อมูลระหว่างหน่วยงานของรัฐโดยใช้เทคโนโลยีดิจิทัลอย่างมั่นคงปลอดภัย รวมทั้งการเปิดเผยข้อมูลภาครัฐผ่านระบบดิจิทัลเพื่อให้การใช้ประโยชน์ในข้อมูลเป็นไปอย่างคุ้มค่า

1.3 ความสอดคล้องยุทธศาสตร์ระดับหน่วยงาน

1.3.1 แผนยุทธศาสตร์กระทรวงมหาดไทย พ.ศ. 2566 – 2570 ยุทธศาสตร์ที่ 4 การพัฒนาองค์กรให้พร้อมรับต่อการเปลี่ยนแปลง

1.3.2 แผนยุทธศาสตร์กรมการปกครอง (พ.ศ. 2566 - 2567) ยุทธศาสตร์ที่ 4 พัฒนาการบริหารองค์กรและบุคลากรตามหลักธรรมาภิบาล ให้มีขีดสมรรถนะสูง ทันสมัยรองรับต่อความเปลี่ยนแปลง

1.3.3 ยุทธศาสตร์ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง ในประเด็นยุทธศาสตร์ : การพัฒนาและบริหารจัดการระบบฐานข้อมูลสารสนเทศให้ทันสมัยและมีประสิทธิภาพ

2. ส่วนราชการ

2.1 ชื่อส่วนราชการ

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง กระทรวงมหาดไทย

2.2 สถานที่ตั้ง

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง อาคาร 3 ชั้น 2 วังไชยา

ถนนนครสวรรค์ แขวงถนนนครไชยศรี เขตดุสิต กรุงเทพฯ 10300

2.3 หัวหน้าส่วนราชการ

นายอรรษิษฐ์ สัมพันธรัตน์ อธิบดีกรมการปกครอง

2.4 ผู้รับผิดชอบโครงการ

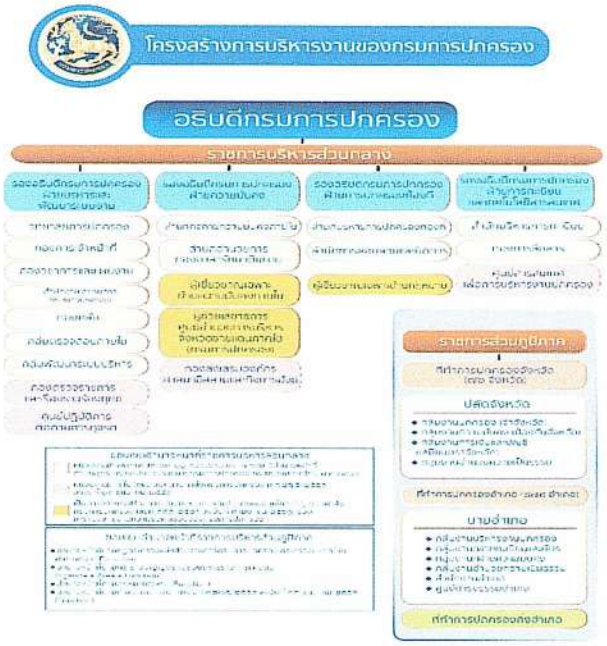
นายก่อเกียรติ แก้วกิ่ง ผู้อำนวยการศูนย์สารสนเทศเพื่อการบริหารงานปกครอง

3. ระบบงานปัจจุบัน

3.1 หน้าที่ความรับผิดชอบของหน่วยงาน

ศูนย์สารสนเทศเพื่อการบริหารงานปกครองเป็นหน่วยงานที่มีภารกิจหลักในการพัฒนาและปรับปรุงระบบสารสนเทศของกรมการปกครอง เพื่อสนับสนุนนโยบายที่กรมการปกครองได้รับมอบหมายจากรัฐบาล กระทรวงมหาดไทย และ ของกรมการปกครอง ให้ดำเนินงานตามนโยบายและภารกิจสำคัญได้อย่างมีประสิทธิภาพ เสนอแนะนโยบายและจัดทำแผนแม่บทกลยุทธ์ และแผนปฏิบัติการเทคโนโลยีสารสนเทศ รวมทั้งกำกับ ติดตาม และประเมินผล บริหารและพัฒนาระบบสารสนเทศ ศึกษา วิเคราะห์ ออกแบบ และประยุกต์ใช้นวัตกรรมระบบสารสนเทศเพื่อพัฒนาการบริหารงานของศูนย์ปฏิบัติการกรม และเป็นศูนย์กลางเครือข่ายข้อมูลสารสนเทศเพื่อการบริหารราชการระดับอำเภอ พัฒนาบุคลากรและจัดทำหลักสูตรฝึกอบรมด้านการใช้เทคโนโลยีสารสนเทศ โปรแกรมการใช้งานที่มีอยู่เดิมให้ทันสมัย ประยุกต์ใช้นวัตกรรมด้านเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อนำไปใช้เป็นเครื่องมือสนับสนุนการบริหารงานแก่ผู้บริหารและเจ้าหน้าที่ผู้ปฏิบัติงาน

3.2 แผนภูมิการแบ่งส่วนราชการ



3.3 ปริมาณงานในปัจจุบัน

ที่	ชื่อระบบ
1	ระบบการสร้างความเข้มแข็งหมู่บ้าน ตามแนวทาง “แผนดินธรรม แผนดินทอง”
2	ระบบการอบรมออนไลน์ของข้าราชการและบุคลากรในสังกัด ปค. บนหน้าเว็บไซต์ของ วช. (หลักสูตรภาษาลาว)
3	ระบบประเมินการบริหารสถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัส
4	ระบบการจัดทำสื่อการเรียนรู้ผ่านระบบอิเล็กทรอนิกส์ (E-learning) (หลักสูตรสืบสวนสอบสวน)
5	ระบบงานสารบรรณอิเลคทรอนิกส์
6	ระบบรายงานผลการผลการดำเนินการตามนโยบาย ลดอบายมุข สร้างสุขให้สังคม
7	ระบบอำเภอคุณธรรม
8	ระบบฐานข้อมูลนามสงเคราะห์และชื่อภูมิศาสตร์ภายใต้ภารกิจของ ปค.
9	ระบบอำเภอบำบัดทุกข์ บำรุงสุข
10	ระบบ ThaiQM
11	ระบบแผนพัฒนาระดับอำเภอ
12	ระบบข้อมูลสารสนเทศเพื่อการบริหารงานซ่อมและสงกำลังบำรุง ของ สส.

13	ระบบหมู่บ้านยั่งยืน
14	ระบบจับกุม
15	Thai QM สำรวจครัวเรือน
16	ระบบ DOPA E-Maps
17	ระบบหนึ่งหมู่บ้าน หนึ่งความดี ร่วมฉลอง 130 ปี
18	ระบบจิตอาสาพระราชทาน

ระบบภายนอกที่จะย้ายเข้ามาที่ VMWare ของ ศสป.

1. เว็บไซต์สำนักกองทั้งหมด (multi.dopa.go.th)
2. เว็บไซต์สารสนเทศสำหรับบุคลากรกรมการปกครอง (intranet.dopa.go.th)
3. ระบบสารบรรณอิล็กทรอนิกส์ (edoc)
4. ระบบ ITA-Amphoe (ระบบประเมินคุณธรรมและความโปร่งใส ในการดำเนินงานของหน่วยงานภาครัฐ สำหรับที่ทำการปกครองอำเภอ)
5. ระบบคำร้องขอย้าย ของกองการเจ้าหน้าที่
6. ระบบ E-Learning กรมการปกครอง
7. ระบบโครงการอำเภอสวยงาม
8. ระบบรายงานผลการดำเนินงานการป้องกันและแก้ไขปัญหายาเสพติด (อส.)
9. ระบบประเมินผู้ผ่านการได้รับความช่วยเหลือจากศูนย์ฟื้นฟูสภาพทางสังคม (อส.)
10. ระบบนิเทศและติดตามการประเมินผลโครงการ (DCAST)
11. ระบบติดตามประเมินผลหมู่บ้านยั่งยืน (Sustainable Village)
12. ระบบรายงานผู้ครอบครองสิ่งเทียมอาวุธปืน
13. ระบบโครงการสร้างความปรองดองสมานฉันท์โดยใช้หลักธรรมทางพระพุทธศาสนา "หมู่บ้านรักษาศีล 5 ขยายผลสู่ หมู่บ้านศีลธรรม"
14. ระบบ @mail.dopa.go.th (สำรองการใช้งานของ workd)
15. ระบบ Tableu (รวบรวมข้อมูลของกรมการปกครอง เพื่อจัดทำ Data Analytics)
16. ระบบบัญชีข้อมูล (Data Catalog) และการเปิดเผยข้อมูลภาครัฐ (Open Data) กรมการปกครอง
17. ระบบอื่นๆ ตามนโยบายของกระทรวงมหาดไทย

3.4 บุคลากรด้านระบบสารสนเทศศูนย์สารสนเทศเพื่อการบริหารงานปกครอง

1. นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ		จำนวน 1 คน
2. เจ้าพนักงานปกครอง ชำนาญการ		จำนวน 1 คน
3. นักวิชาการคอมพิวเตอร์ ชำนาญการ		จำนวน 8 คน
4. นักวิชาการคอมพิวเตอร์ ปฏิบัติการ		จำนวน 2 คน
5. เจ้าหน้าที่ปกครอง ชำนาญงาน		จำนวน 1 คน
6. เจ้าหน้าที่ธุรการ ชำนาญงาน		จำนวน 3 คน
7. เจ้าหน้าที่เครื่องคอมพิวเตอร์ ปฏิบัติงาน		จำนวน 1 คน
7. พนักงานราชการ		จำนวน 7 คน
8. ลูกจ้างเหมาบริการ		จำนวน 2 คน
	รวม	จำนวน 26 คน

4. ระบบงานใหม่

4.1 วัตถุประสงค์และเป้าหมาย

4.1.1 วัตถุประสงค์

1) เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามด้านไซเบอร์และเตรียมความพร้อมในการรับมือกับภัยคุกคามทั้งภายในและภานนอก

2) เพื่อวิเคราะห์และประเมินความเสี่ยงของระบบสารสนเทศทำการทดสอบการเจาะหาช่องโหว่เครือข่ายจากภายในและภายนอกพร้อมทั้งรับข้อเสนอแนะในการปรับปรุงระบบความปลอดภัยที่เกี่ยวข้อง

3) เพื่อเพิ่มความปลอดภัย และเพิ่มการป้องกันจากการโจมตีของผู้ไม่ประสงค์ดี

4) สร้างความหน้าเชื่อถือและเพิ่มความมั่นใจในการใช้งาน

4.1.2 เป้าหมาย

จัดหาระบบตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) 1 ระบบ สำหรับการประเมินความมั่นคงปลอดภัยของระบบสารสนเทศภายในหน่วยงานเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบต่างๆ โดยผู้ตรวจสอบภายในหน่วยงานของ ปค. (โปรแกรมทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่)

4.2 ประเภทการขออนุมัติ

ดำเนินการจัดจ้างบริษัทที่มีความชำนาญในการให้บริการโปรแกรมทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว จำนวน 1 ระบบ โดยมี license พร้อมการรับประกัน 12 เดือน โดยใช้วิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

4.3 การวิเคราะห์ออกแบบระบบงาน และคุณลักษณะของอุปกรณ์คอมพิวเตอร์ที่จัดหาในโครงการ

โครงการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ (Penetration Testing) 1 ระบบ มีคุณสมบัติอย่างน้อยดังนี้

4.3.1 ระบบที่นำเสนอต้องเป็นซอฟต์แวร์ ที่ออกแบบมาทำการทดสอบการเจาะระบบเครือข่าย โดยเฉพาะ และมีลิขสิทธิ์สำหรับผู้ทำการทดสอบจำนวน 1 user เป็นอย่างน้อย

4.3.2 สามารถติดตั้งบนระบบปฏิบัติการ windows ได้เป็นอย่างน้อย

4.3.3 สามารถบริหารจัดการผ่านทาง web browser และ GUI ได้เป็นอย่าน้อย

4.3.4 สามารถตรวจหา TCP/UDP Service ที่กำลังทำงานอยู่บนเครื่องเป้าหมายได้

4.3.5 สามารถทดสอบการเจาะระบบเครื่องเป้าหมายได้ทั้งแบบ Single IP และ IP Range ได้แบบ Unlimited IP Address

4.3.6 มีความสามารถสอบเจาะระบบเครื่องเป้าหมายได้แบบอัตโนมัติ (Automated)

4.3.7 รองรับการตรวจหาช่องโหว่ที่ระบบเครือข่าย และระบบปฏิบัติการภายในหน่วยงาน

4.3.8 รองรับการตรวจหาช่องโหว่ที่เว็บแอพพลิเคชันที่ถูกพัฒนาขึ้นมาทั้งก่อนและหลังใช้งาน

4.3.9 สามารถปรับแต่งระดับความรุนแรงในการทดสอบเจาะระบบได้ (CVE Number) ได้

4.3.10 สามารถทดสอบเจาะรหัสกับ service ต่างๆ เช่น SMB, PostgreSQL, DB2, MY SQL, MSSQL, HTTP, SSH, Telnet, FTP, POP3, VNC และ SNMP ได้เป็นอย่างน้อย

4.3.11 มี built-in dictionary attack และรองรับการปรับแต่ง หรือเพิ่มรหัสผ่านที่ใช้ทดสอบการเจาะรหัสได้

4.3.12 ภายหลังการตรวจสอบมีความสามารถในการทำงานต่างๆ อย่างน้อยดังนี้ เช่น การเก็บข้อมูลจากเครื่องที่ทดสอบ (Gather) การสร้าง Session หรือ ติดตั้ง Agent กับเครื่องที่ทดสอบผ่านช่องโหว่ที่ตรวจพบ, การแสดงรายการ File System และการส่งชุดคำสั่ง (Command shell) ไปยังเครื่องที่ทดสอบได้

4.3.13 สามารถทดสอบการติดตั้งโปรแกรมไม่พึงประสงค์โดยการส่งโปรแกรม (Deploying Agents) หรือ Post-Exploitation Module ไปยังเครื่องที่ทดสอบได้

4.3.14 สามารถสร้างแบบทดสอบพฤติกรรมแบบ Phishing email ของผู้ใช้ด้านความปลอดภัยคอมพิวเตอร์ (Social Engineering) ทั้งในรูปแบบ Web Browser และ Email Client ได้

4.3.15 สามารถออก Dashboard หรือรายงานการทดสอบหาช่องโหว่ได้ และแสดงรายการช่องโหว่/ข้อตรวจพบ , URL/IP address ที่มีช่องโหว่/ข้อตรวจพบ

4.3.16 สามารถสร้างรายงานได้หลากหลายรูปแบบ เช่น Activity Report, Vulnerability Report, หรือ Compromised, Web Apps Report, FISMA Report, PCI Report, MITER ATT&CK framework, NIST framework เป็นต้น

4.3.17 สามารถออกรายงานตามรูปแบบไฟล์ PDF หรือ WORD ได้เป็นอย่างน้อย

4.3.18 สามารถเก็บรายงานที่สร้างไว้ในตัวอุปกรณ์ (local) หรือส่งออกทาง Email ได้

4.3.19 สามารถอัพเดต Software และฐานข้อมูลการทดสอบช่องโหว่จากผู้ผลิตได้ตลอดระยะเวลาการรับประกัน

4.3.20 ความสามารถทดสอบการเจาะระบบกับ Web Application รองรับการทำงานได้ดังนี้

1) สามารถทดสอบ และวิเคราะห์โดยครอบคลุม OWASP Top 10 เวอร์ชั่นล่าสุดได้

2) สามารถทำ Web crawling กับเว็บไซต์ภายในหน่วยงานได้

3) สามารถทดสอบ URL หรือ Parameter ของเว็บไซต์โดยเทคนิคต่างๆ เช่น SQL Injection หรือ Cross Site Scripting เป็นต้นได้

4.3.21 ผู้ขายจะต้องมีหนังสือการรับประกันคุณภาพผลิตภัณฑ์จากเจ้าของผลิตภัณฑ์หรือสาขาของเจ้าของผลิตภัณฑ์ในประเทศไทย

4.3.22 มีลิขสิทธิ์ถูกต้องตามกฎหมายจากเจ้าของผลิตภัณฑ์ และสิทธิ์การใช้งานไม่น้อยกว่า 1 ปี

4.3.23 ผู้ขายจะต้องจัดให้มีการอบรมการเจาะระบบโดย software ที่จัดซื้อเพื่อป้องกัน แบบเชิงรุก ให้กับบุคลากรของกรมการปกครอง ไม่น้อยกว่า 3 คน จำนวน 1 หลักสูตร

4.4 สถานที่ติดตั้ง

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง วังไชยา

4.5 ค่าใช้จ่าย

งบประมาณรายจ่าย ประจำปีงบประมาณ พ.ศ. 2568 งบลงทุนในวงเงิน 2,284,450 บาท

4.6 แผนการดำเนินงานและระยะเวลาดำเนินงาน ระยะเวลาร่วม 120 วัน นับจากวันทำสัญญา

กิจกรรม	จำนวนวัน												หมายเหตุ
	10	20	30	40	50	60	70	80	90	100	110	120	
1. ขออนุมัติโครงการ	←	→											
2. ดำเนินการจัดหาผู้รับจ้าง		←	—	→									
3. ลงนามในสัญญา				←	→								
4. ติดตั้งส่งมอบ				←	—	—	—	—	—	→			
5. ตรวจรับ/ทดสอบระบบ										←	—	→	

5. ผลประโยชน์ที่คาดว่าจะได้รับ

5.1 ตัวชี้วัดเชิงปริมาณ มีการตรวจสอบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ 1 ระบบ ด้วยวิธีการทดสอบเจาะหาช่องโหว่ทำให้ระบบเทคโนโลยีสารสนเทศของ ปค. เป็นไปอย่างเหมาะสม

5.2 ตัวชี้วัดเชิงคุณภาพ ร้อยละของความพึงพอใจของผู้ปฏิบัติงานในสังกัด ปค. ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัยและมีประสิทธิภาพ

5.3 ระบบเทคโนโลยีสารสนเทศของ ปค. มีเสถียรภาพและประสิทธิภาพ ความมั่นคงปลอดภัยด้านสารสนเทศได้มาตรฐานและป้องกันภัยคุกคามต่างๆ และสามารถดำเนินงานได้อย่างต่อเนื่อง

ภาคผนวก ข.

บริษัท โซ บี อิท โซลูชั่นส์ จำกัด (สำนักงานใหญ่)
SO BE IT SOLUTIONS CO., LTD. (HEAD OFFICE)
[illegible]
20/1 SOI RAMKHAMHAENG 131, SAPHAN SUNG, SAPHAN SUNG, BANGKOK 10240
โทร : 085-914-9114 เลขประจำตัวผู้เสียภาษีอากร : 0105564067800

ใบเสนอราคา / QUOTATION

ลูกค้า : เรียน อธิบดีกรมการปกครอง
ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง
ถนนนครสวรรค์ แขวงสี่แยกมหานาค เขตดุสิต กทม . 10300
เลขประจำตัวผู้เสียภาษี : 0994000162626

วันที่ (DATE)	
เลขที่ใบเสนอ (QUOTATION No.)	DCQ6611009
ยืนราคา (VALIDITY)	15 วัน
เงื่อนไขการชำระเงิน (PAYMENT TERM)	30 วัน
กำหนดส่งสินค้า (DELIVERY DATE)	90 วัน
การรับประกัน (WARRANTY)	1 ปี

ลำดับ ITEM	รหัสสินค้า P/N	รายการ DESCRIPTION	จำนวน QUANTITY	ราคา (บาท) / หน่วย UNIT PRICE (BAHT)	จำนวนเงิน (บาท) AMOUNT (BAHT)
		Penetration Test Software and Service			
		โปรแกรมทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่ในระบบเน็ตเวิร์ก			
1	CT00770	ยี่ห้อ Core Impact รุ่น Enterprise User License	1 License	2,000,000.00	2,000,000.00
		Subscription 12 months			
		ความสามารถในกระบวนการทดสอบ			
		- การทดสอบเครือข่าย เปิดเผยและใช้ประโยชน์จากจุดอ่อนด้านความปลอดภัยภายในโครงสร้างพื้นฐานของคุณ			
		- การทดสอบฝั่งไคลเอ็นต์ ทดสอบความแข็งแกร่งของผู้ใช้ของคุณด้วยการโจมตีทางวิศวกรรมสังคม			
		- การทดสอบ WiFi ประเมินความปลอดภัยของเครือข่ายไร้สายโดยใช้จุดเข้าใช้งานปลอม			
		- การทดสอบแอปพลิเคชันเว็บ ประเมินความปลอดภัยของแอปพลิเคชันเว็บโดยกำหนดเป้าหมายหน้าเว็บและ URL			
		- Add-On Exploit Pack Integration* ชุดการหาประโยชน์จาก Excraft ที่ออกแบบมาสำหรับ SCADA, อุปกรณ์ IoT			
		คุณสมบัติของโปรแกรม			
		- การทดสอบการเจาะระบบอย่างรวดเร็ว ระบบอัตโนมัติที่สามารถเข้าถึงได้ซึ่งออกแบบมาเพื่อเพิ่มประสิทธิภาพการใช้ทรัพยากรความปลอดภัยของคุณ			
		- โมดูลทดสอบ สร้างงานของคุณเองเพื่อแนวทางปฏิบัติที่มากขึ้น			
		- การรายงาน การรายงานอัตโนมัติเพื่อให้มั่นใจถึงความสม่ำเสมอ เพิ่มประสิทธิภาพ และสร้างบันทึกกิจกรรมทั้งหมดอย่างละเอียด			
		- บูรณาการ ตรวจสอบเครื่องสแกนช่องโหว่และรวมศูนย์การทดสอบปากกาผ่านความสามารถในการทำงานร่วมกันกับ Metasploit, Plexrac และ Cobalt Strike			
		- ขอบเขตการทดสอบ IP แบบไม่จำกัด ทดสอบ IP ได้มากเท่าที่คุณต้องการ			
		- Pivot ภายในเครื่องจากเครื่องที่ถูกบุกรุก			
		- Cloud Cypher Access ส่งข้อมูลรับรองที่เข้ารหัสไปยังบริการถอดรหัสรหัสผ่านออนไลน์ของเราโดยอัตโนมัติ			
		- อินเทอร์เฟซเว็บ อินเทอร์เฟซเบราว์เซอร์ที่ช่วยให้คุณทำงานผ่าน HTTPS			
		- REST API ขยายฟังก์ชันการทำงานสำหรับการผสานรวมเพิ่มเติม			
		- ความสามารถในการทำงานเป็นทีม ได้ตอบในพื้นที่ทำงานทั่วไปเพื่อแบ่งปันข้อมูลและมอบหมายงานการทดสอบ			
	Service	Core Impact Installation & traning Services - Remote	1 Service	135,000.00	135,000.00
		- ลงโปรแกรม Core Impact ติดตั้งและปรับแต่งคุณสมบัติ ในเครื่องคอมพิวเตอร์แม่ข่าย			
		- ทำการตรวจ ค้นหาช่องโหว่ และสร้างแบบจำลองเพื่อทดสอบเจาะระบบ			
		- อบรมการใช้งานโปรแกรม			
		- เก็บข้อมูลหลังทำการทดลอง ในรูปแบบเอกสาร			
		- จัดทำรายการและข้อแนะนำ			

จำนวนเงิน	2,135,000.00
ส่วนลด	-
รวมราคาทั้งสิ้น	2,135,000.00
ภาษีมูลค่าเพิ่ม VAT 7%	149,450.00
จำนวนเงินทั้งสิ้น	2,284,450.00

สองล้านสองแสนแปดหมื่นสี่พันสี่ร้อยห้าสิบบาทถ้วน

ท่านสามารถยืนยันการสั่งซื้อได้ที่นี่

เราเข้าใจในการเสนอราคาและเงื่อนไขข้างต้นและเราขอยืนยันคำสั่งซื้อนี้

Authorized Signature : _____

( )

Date : _____

คุณเดชา ว่องพระคุณ
085 914 9114
[illegible]
ผู้เสนอราคา

บริษัท เค ที โปรเฟสชั่นแนล จำกัด
K T Professional Co.,Ltd

4/1523 หมู่ที่ 4 ถนนเสรีไทย แขวงคลองกุ่ม เขตบึงกุ่ม กรุงเทพฯ 10240
4/1523 Moo 4 Serithai Rd. Klong Kum, Beung Kum, Bangkok 10240
Tel./Fax (662) 704 8482 เลขประจำตัวผู้เสียภาษี 0105547036195

Quotation/Order Acknowledgement Ref. No. : SSW2311004

ใบเสนอราคา/ใบยืนยันการสั่งซื้อ

We are pleased to submit you the following quotation and offer to sell the products or service described in at price, items and terms stated.
บริษัทฯ มีความยินดีในการเสนอราคาเพื่อขายผลิตภัณฑ์หรือบริการแด่ท่านตามราคาและเงื่อนไขที่ระบุไว้ในใบเสนอราคาฉบับนี้

CUSTOMER INFORMATION	QUOTATION INFORMATION
ลูกค้า เรียน อธิบดีกรมการปกครอง ที่อยู่ กรมการปกครอง ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง ถนนอัษฎางค์ แขวงวัดราชบพิธ เขตพระนคร กทม. 10200 เลขประจำตัวผู้เสียภาษี 0994000162626	Delivery/การส่งของ : 90 วัน Warranty/การรับประกัน : 1 ปี Payment/การชำระเงิน : 30 วัน Validity/การยืนราคา : 15 วัน Currency : BAHT

ITEM รายการ	PART NO. รหัสสินค้า	DESCRIPTION รายละเอียด	QTY จำนวน	หน่วย	UNIT PRICE ราคาต่อหน่วย	NET PRICE ราคารวม
1	CT00770	Penetration Test Software and Service Core Impact - Enterprise User License Subscription 12 months	1	License	2,100,000.00	- 2,100,000.00
	Service	Core Impact Installation & Ytaning Services - Remote - Installation of Core Impact - Product Configuration - Scan run test simulation - Quick Product Traning - Document - Report - Total of 6 mandays	1	Service	160,000.00	160,000.00
		'บริการทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่ ตามมาตราฐานการทดสอบ OWASP, SANS, NIST,PETS บริการประกอบด้วยคุณลักษณะและรายละเอียดดังนี้ - การทดสอบระบบประเภท Black Box - ทดสอบการเจาะระบบ 2 ครั้ง (initial and re-test) - การนำผลการวิเคราะห์ระดับความเสี่ยงที่ได้มาจัดทำรายงาน และจัดทำแนวทาง				

สองล้านสี่แสนหนึ่งหมื่นแปดพันสองร้อยบาทถ้วน	Total	2,260,000.00
	VAT 7%	158,200.00
	Grand Total	2,418,200.00

Customer

Price and terms as above are understood and we confirm this order.
เราเข้าใจในการเสนอราคาและเงื่อนไขข้างต้นและเราขอยืนยันคำสั่งซื้อนี้

Authorized Signature : _____

( )

Date : _____

K T Professional Co.,Ltd.

We look forward to give you our best service.
บริษัทหวังเป็นอย่างยิ่งว่าจะได้บริการท่านในเร็ววันนี้

Authorized by:

(นางสาวกนกวรรณ วังศเมฆีกูร)
e-Mail : w_kanokwan@hotmail.com
Mobile : 081-615-4596

Point IT Consulting Co.,Ltd.
19 Soi Supapong 1 Split 6, Kweng Nongbon,Khet Prawet, Bangkok 10250, Thailand.
Tel : +66 (0) 2348-4792, Fax : +66 (0)2348-4793

Customer เรียน อธิบดีกรมการปกครอง
ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง
ถนนนครสวรรค์ แขวงสี่แยกมหานาค เขตดุสิต กทม. 10300
เลขประจำตัวผู้หักภาษี : 0994000162626

QUOTATION
Date :
Our Ref. No. SUW0021123

We are pleased to submit you the following descriptions and the prices as follows:

Product	Description	Qty.	Per Unit Baht	Amount Baht	Warranty Period
	Penetration Test Software and Service				
CT00770	Core Impact - Enterprise User License Subscription 12 months	1	2,250,000.00	2,250,000.00	1 Year
Service	Core Impact Installlation & Ytaning Services - Remote - Installation of Core Impact - Product Configuration - Scan run test simulation - Quick Product Traning - Document - Report - Total of 6 mandays	1	160,000.00	160,000.00	
	'บริการทดสอบการบุกรุกระบบด้วยการจำลองเหตุการณ์เพื่อให้ทราบถึงผลกระทบของช่องโหว่ ตามมาตราฐานการทดสอบ OWASP, SANS, NIST,PETS บริการประกอบด้วยคุณลักษณะและรายละเอียดดังนี้ - การทดสอบระบบประเภท Black Box - ทดสอบการเจาะระบบ 2 ครั้ง (initial and re-test) - การนำผลการวิเคราะห์ระดับความเสี่ยงที่ได้มาจัดทำรายงาน และจัดทำแนวทาง				
	SUB TOTAL			2,410,000.00	
	Value added Tax		7.00%	168,700.00	
	GRAND TOTAL			2,578,700.00	

Term & Condition
- The price is subject to chang without prior notics
- Delivery date : within 90 Days

กำหนดชำระเงิน ตามเงื่อนไขราชการ
กำหนดยืนราคา ภายใน 15 วันนับจากวันเสนอราคา

Miss Woraluck Khunsuwanchai
Account Executive

Confirmed By: ( )

Date :

ภาคผนวก ค.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ด่วนที่สุด

ที่ สกมช ๐๖๐๐/ว๕๐๑๔

๓๐ พฤศจิกายน ๒๕๖๖

เรื่อง เร่งรัดการจัดส่งผลสรุปรายงานการดำเนินการตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

เรียน อธิบดีกรมการปกครอง

อ้างถึง หนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ สกมช ๐๖๐๐/ว๓๐๑๖ ลงวันที่ ๑๑ สิงหาคม ๒๕๖๖

ตามหนังสืออ้างถึง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีหนังสือที่ สกมช ๐๖๐๐/ว๓๐๑๖ ลงวันที่ ๑๑ สิงหาคม ๒๕๖๖ เรื่อง แจ้งเตือนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และขอเชิญเข้าร่วมประชุมชักซ้อมความเข้าใจเกี่ยวกับการดำเนินการตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประจำปี ๒๕๖๖ ความรายละเอียดแจ้งแล้ว นั้น

เนื่องจากหน่วยงานของท่านยังมิได้จัดส่งผลสรุปรายงานการดำเนินการดังกล่าว สกมช. จึง**ขอความร่วมมือในการเร่งรัดการจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานฯ ภายในวันที่ ๓๐ มกราคม ๒๕๖๗** เพื่อที่สำนักงานฯ จะได้รวบรวมผลสรุปรายงานการดำเนินการดังกล่าว เสนอต่อคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) พิจารณาสั่งการและให้ความเห็นชอบก่อนนำเสนอต่อนายกรัฐมนตรีต่อไป หากไม่สามารถจัดส่งผลสรุปรายงานการดำเนินการดังกล่าวได้ทันภายในระยะเวลาที่กำหนด ขอให้มีหนังสือแจ้งเหตุผลมายัง สกมช. ภายในวันดังกล่าว ทั้งนี้ สกมช. ได้มอบหมายให้ นางสาวแสงระวี ศรีจำรัส หมายเลขโทรศัพท์ ๐ ๒๕๐๒ ๗๘๒๖ เป็นผู้ประสานงาน

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการ จะขอบคุณยิ่ง

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
โทรศัพท์ ๐ ๒๕๐๒ ๗๘๒๖
ไปรษณีย์อิเล็กทรอนิกส์ cii@ncsa.or.th

CORE SECURITY

Core Impact Licenses Options

Core Impact customers can attend online for self-paced learning

Core Impact License Options	Basic	Pro	Enterprise
TESTS			
Network Testing Uncover and exploit security weaknesses within your infrastructure	●	●	●
Client Side Testing Test the strength of your users with social engineering attacks		●	●
Wifi Testing Evaluate the security of wireless networks using fake access points			●
Web Application Testing Assess the security of web applications by targeting web pages and urls			●
Add-On Exploit Pack Integration* Excraft exploitation packs designed for SCADA, IoT devices, or medical software are available for purchase			●
FEATURES			
Rapid Penetration Tests Accessible automations designed to optimize the use of your security resources	●	●	●
Test Modules Build your own individual tasks for a more hands on approach	●	●	●

CORE SECURITY

Reporting Automated reporting to ensure consistency, increase efficiency, and create a thorough record of all activity			
Integrations Validate vulnerability scanners and centralize pen testing through interoperability capabilities with Metasploit, Plextrac, and Cobalt Strike			
Unlimited IP Testing Scope Test as many IPs as you need			
Pivoting Pivot locally from a compromised machine			
CloudCypher Access Automatically submit encrypted credentials to our online password cracking service			
Web Interface A browser interface that allows you to work over HTTPS			
REST API Extend functionality for additional integrations			
Teaming Capabilities Interact in a common workspace to share data and delegate testing tasks			
Support Get assistance from the talented global support team	Customer Portal and email support	Customer Portal and email support	Phone, Customer Portal and email support

CORE SECURITY

About Core Security Corporation

Core Security provides companies with the security insight they need to know who, how, and what is vulnerable in their organization. The company's threat-aware, identity & access, network security, and penetration testing solutions provide actionable insight and context needed to manage security risks across the enterprise. This shared insight gives customers a comprehensive view of their security posture to make better security remediation decisions. Better insight allows organizations to prioritize their efforts to protect critical assets, take action sooner to mitigate access risk, and react faster if a breach does occur.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and Asia. To learn more, contact Core Security at (678) 304-4500 or info@coresecurity.com.

p: (678) 304-4500 | info@coresecurity.com | www.coresecurity.com

coresecurity
by HelpSystems

FORTRA

Core Impact

Penetration testing software to safely uncover and exploit security weaknesses

Core Impact uses the same techniques as today's threat actors to efficiently test the security of an IT infrastructure to help minimize risk and protect valuable assets. With the help of guided automations, organizations can discover, test, and report in just a few simple steps.

Simple Enough for Your First Test, Powerful Enough for the Rest

Core Impact's Rapid Penetration Tests (RPTs) are intuitive wizards that enable testers to swiftly conduct penetration tests. Users can efficiently execute common tasks, saving time while providing a consistent, repeatable process for their testing infrastructure. Additionally, Core Impact allows you to quickly re-test exploited systems to verify that remediation measures or compensating controls are effective and working.

Leverage a Robust Library of Core Certified Exploits

Using an up-to-date library of commercial-grade exploits, developed and tested by Core Security's own cybersecurity experts, Core Impact reveals how chains of exploitable vulnerabilities open paths to your organization's mission-critical systems and assets. In addition to internally written exploits, Core Security partners with ExCraft Labs to provide add-on packs for supplementary SCADA, medical, and IoT exploits, on top of the standard exploits included with Core Impact.

Centralize Your Pen Testing Toolkit and Maximize Testing Visibility

Gather information, exploit systems, and generate reports, all in one place. Every phase of the penetration test process can be executed and managed from a single console with an intuitive dashboard. Instead of switching back and forth between tools, additional solutions can also be integrated or incorporated to further expand your testing program, such as Cobalt Strike, OST, Metasploit, PowerShell Empire, and Plextrac. This centralization not only simplifies the testing process, not having to manually compile documentation, but it also makes reporting more consistent and efficient.

PRODUCT SUMMARY

KEY FEATURES

- Intuitive automation for deploying advanced level tests
- Extensive and reliable library of certified exploits
- Multi-vector testing capabilities
- Teaming capabilities in a collaborative workspace
- Tailored reporting to build remediation plans
- Powerful integrations with other pen testing tools and more than 20 vulnerability scanners
- Robust safety features, including fully encrypted, self-destructing agents

PLATFORMS MONITORED

- Operating Systems including Windows, Linux, and Mac
- Cloud (Public, Private, Hybrid)
- Databases
- Web Services
- Network Appliances
- Software Applications
- Your Critical Data

SYSTEM REQUIREMENTS

- Windows 10 Enterprise 64 bit
- Windows 10 Pro 64 bit
- Windows Server 2016 Standard

For those that prefer a more visual experience, users can enjoy Core Impact's interactive attack map as their central workspace. This network graph view displays a real-time overview of attack chains, pivoting and any other activities completed during testing, providing visual insight that allows security teams to better determine the best path forward in the testing engagement.

Common Core Impact Use Cases

Core Impact offers diverse testing functionality in order to provide thorough coverage and security insight so organizations know who, how, and what is vulnerable in their IT environments.

Proving Compliance with Industry Regulations

Multiple regulations require organizations have regular assessments of their security infrastructure to ensure sensitive data is properly protected. Core Impact provides an easy to follow and established automated framework that can support industry requirements and standards, including PCI-DSS, CMMC, GDPR, and NIST. For example, the NIST reports map alignment with both the MITRE ATT&CK framework and NIST's catalog of security and privacy controls. Additionally, Core Impact's reporting capabilities can help prove adherence to regulations during internal or external audits.

Conduct Network and Web Application Tests

Accurately identify and target internal information systems for network penetration testing. Core Impact can help exploit vulnerabilities in critical networks, systems, hosts, and devices by imitating an attacker's methods of access and manipulating data, as well as testing defensive technologies' ability to stop attacks.

Run web application penetration tests to find weaknesses through detailed web crawling, pivoting attacks to web servers, associated databases, and backend networks to confirm exploitability.

Conducting Ransomware and Phishing Simulations for Increased Security Awareness

Easily deploy phishing campaigns for client-side social engineering tests to discover which users are susceptible and what credentials can be harvested. Use the step-by-step process to create emails, select targets, and choose between browser redirects or web page clones. Challenge users with more sophisticated, tailored spear-phishing emails that are harder to identify as fake.

Pair phishing campaigns with the ransomware simulator and mimic the behavior of multiple ransomware families, encrypting user-specified files using a fully reversible symmetric key. Security teams can create and leave an explanatory README file once the exercise has been completed.

Validating Vulnerabilities Surfaced Through Scanners

Core Impact's one-step test can quickly validate the results of over 20 different third-party scanners, including beSECURE, Frontline VM, Nessus and BurpSuite. After you complete a scan against your environment, Core Impact can evaluate the scan's output and provide a prioritized validation of your infrastructure's weaknesses.

Vulnerability Scan Validation*

- Acunetix Web Vulnerability Scanner
- beSECURE
- Burp Suite Professional
- Cenzic
- Frontline VM
- GFI LANguard
- HP WebInspect
- IBM Enterprise Scanner
- IBM Internet Scanner
- IBM Rational AppScan
- McAfee Vulnerability Manager (formerly McAfee Foundstone)
- Microsoft Baseline
- nCircle
- Nessus
- Nexpose
- Nmap
- NTOSpider
- Patchlnk VMS
- Qualys Guard
- Qualys Web Application Scanner
- Retine
- SAINT
- STAT Guardian
- Tenable Security Center
- Tripwire IP360

* A vulnerability scanner is not required to use Core Impact