แบบ ICOP1

รายงานการไปราชการ ประชุม สัมมนา ศึกษา ฝึกอบรม ปฏิบัติการวิจัย ดูงาน ณ ต่างประเทศ และการปฏิบัติงานในองค์การระหว่างประเทศ

ส่วนที่๑ ข้อมูลทั่วไป

๑.๑ ชื่อ-สกุล.....นายกฤษฎา ถิ่นทับปุด.....

๑.๒ ตำแหน่ง ....นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ.....

๑.๓ สังกัด .....กองยุทธศาสตร์และแผนงาน.....

๑.๔ชื่อเรื่อง/หลักสูตร

(ภาษาไทย) .....

(ภาษาอังกฤษ) ..... Technical Meeting on Conducting Computer Security Exercises for Nuclear Security.....

เพื่อ ☐ ศึกษา ☐ ฝึกอบรม ☐ดูงาน

☒ ประชุม / สัมมนา ☐ ปฏิบัติงานวิจัย ☐ ไปปฏิบัติงานในองค์การระหว่าง

แหล่งให้ทุน .....ทบวงการพลังงานปรมาณูระหว่างประเทศ (IAEA) .....

สถานที่ (หน่วยงาน/ประเทศ) .....IAEA/สาธารณรัฐออสเตรีย.....

ระหว่างวันที่ .....๓ ๖ กันยายน ๒๕๖๑.....

รวมระยะเวลาการรับทุน .....๔ วัน.....

ส่วนที่ ๒ข้อมูลที่ได้รับจากการศึกษา ฝึกอบรม ดูงาน ประชุม/สัมมนา ปฏิบัติการวิจัย และการไปปฏิบัติงานในองค์การระหว่างประเทศ (โปรดให้ข้อมูลในเชิงวิชาการ หากมีรายงานแยกต่างหาก)

๒.๑ วัตถุประสงค์

เพื่อเป็นเวทีประชุมระหว่างประเทศในการหารือเกี่ยวกับประสบการณ์ของผู้เข้าร่วมการประชุม และระบุถึงแนวทางปฏิบัติที่ดีในการซักซ้อมความมั่นคงทางคอมพิวเตอร์ ซึ่งเป็นกิจกรรมที่ประกันความมั่นคงทางนิวเคลียร์

โดยประเทศที่เข้าร่วมการประชุมครั้งนี้ ประกอบด้วย ประเทศอาร์เจนตินา อาร์เมเนีย เบลเยียม บราซิล บัลแกเรีย แคนาดา ชิลี จีน อียิปต์ ฝรั่งเศส เยอรมัน กานา ฮังการี อินเดีย อินโดนีเซีย อิหร่าน ญี่ปุ่น เกาหลีใต้ ลิเบีย มาเลเซีย โมรอคโค เนเธอร์แลนด์ ไนจีเรีย ปากีสถาน โรมาเนีย รัสเซีย เซอร์เบีย สโลวาเกีย สวิสเซอร์แลนด์ ไทย ตุรกี สหรัฐอาหรับเอมิเรตส์ อังกฤษ สหรัฐอเมริกา และเวียดนาม .. ....

๒.๒ เนื้อหา (โดยย่อ)

สรุปสาระสำคัญของการประชุมวิชาการในครั้งนี้ มีดังต่อไปนี้

การประชุมวิชาการนี้เพื่อแนะนำเกี่ยวกับกรอบการดำเนินในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Threat Framework) และการใช้แนวทางการดำเนินงานในการพัฒนาสถานการณ์จำลอง (การเตรียมการ ข้อตกลง การนำเสนอ ผลกระทบและผลลัพธ์) โดยประเทศเกาหลีใต้ เนเธอร์แลนด์ และสวีเดน ได้แบ่งปันประสบการณ์เกี่ยวกับการซักซ้อมการเตรียมพร้อมด้านความมั่นคงปลอดภัยทางนิวเคลียร์และไซเบอร์ให้กับผู้เข้าร่วมประชุม

นอกจากนี้ การประชุมวิชาการได้มุ่งเน้นการพัฒนาสถานการณ์จำลอง โดยเริ่มจากการพัฒนา Scenario I (การระบุ และเลือกช่องโหว่ของของระบบ) จากนั้นจึงพัฒนา Scenario II (การพัฒนาสถานการณ์ที่น่าเชื่อถือ โดยพิจารณาจากลักษณะการคุกคาม และการวิเคราะห์รูปแบบและกระบวนการ)

จากนั้นได้แบ่งผู้เข้าร่วมการประชุมออกเป็นกลุ่มต่าง ๆ จำนวน ๔ กลุ่ม เพื่อดำเนินการตามสถานการณ์จำลองในหัวข้อต่าง ๆ ได้แก่ การก่อวินาศกรรม การเคลื่อนย้ายวัสดุนิวเคลียร์ ความปลอดภัยระหว่างการขนส่ง และช่องโหว่ของข้อมูลที่สำคัญ และนำเสนอการจัดการในสถานการณ์จำลองดังกล่าวในสามมุมมอง คือ ผู้โจมตี ผู้พิทักษ์ และผู้สังเกตการณ์ที่เป็นกลาง

IAEA ได้จัดทำเอกสารทางเทคนิคเพื่อเป็นแนวทางสำหรับประเทศสมาชิกในการบริหารจัดการตามสถานการณ์ซักซ้อมความมั่นคงปลอดภัยทางนิวเคลียร์และไซเบอร์ โดยเอกสารทางเทคนิคนี้จะรวมถึง

๑. การใช้กรอบการดำเนินการเกี่ยวกับภัยคุกคามทางไซเบอร์ในการสร้างสถานการณ์จำลอง

๒. คำแนะนำเฉพาะสำหรับการใช้แบบฝึกหัด เพื่อสร้างความเข้าใจเกี่ยวกับวิธีการสร้างองค์ประกอบที่จำเป็นในการพัฒนาสถานการณ์จำลองทางนิวเคลียร์และไซเบอร์

๓. กรอบการประเมินผลภายหลังจากการซักซ้อมสถานการณ์ เพื่อให้เข้าใจถึงประสิทธิภาพของสถานการณ์ที่ใช้ในระหว่างการทดสอบ

มีข้อเสนอแนะจากที่ประชุมโดยพิจารณาจากแหล่งข้อมูลที่ IAEA ให้การสนับสนุนการพัฒนาสถานการณ์ซักซ้อมเกี่ยวกับความมั่นคงปลอดภัยทางนิวเคลียร์และไซเบอร์ ดังต่อไปนี้

การประเมินภัยคุกคาม: ผู้เข้าร่วมประชุมได้ขอให้ IAEA สนับสนุนการดำเนินการประเมินภัยคุกคาม โดยรวมถึงการพัฒนา และทดสอบกรอบการดำเนินการประเมินภัยคุกคาม เช่น การกำหนดลักษณะผู้คุกคาม การจัดเก็บและจัดหมวดหมู่ความสามารถของผู้คุกคาม และระบุความเป็นไปได้ที่ผู้คุกคามจะปฏิบัติตามบทบาทที่กำหนดกับเป้าหมายที่ต้องการ

บัญชีรายการสถานการณ์จำลอง: ผู้เข้าร่วมประชุมขอให้ IAEA จัดทำและปรับปรุงบัญชีรายการสถานการณ์ภัยคุกคามทางนิวเคลีย์และไซเบอร์เพื่อใช้ในการซักซ้อม โดยบัญชีรายการนี้จะรวมถึงรูปแบบของสถานการณ์ที่จัดกลุ่มที่ขึ้นอยู่กับชนิดของเป้าหมาย และแรงจูงใจและความสามารถของผู้คุกคาม

ICS SCADA Repository, ICS ATT&CK, STIX และ TAXI: ที่ประชุมได้ขอให้ประเทศสมาชิกมีสิทธิเข้าถึงพื้นที่เก็บข้อมูล ICS/SCADA ที่มีรูปแบบการคุกคามที่เกี่ยวข้องกับอุปกรณ์ ICS/SCADA ของ IAEA รวมถึงการบูรณาการข้อมูลเกี่ยวกับกระบวนการ ICS ATT&CK และภัยคุกคามตามมาตรฐาน STIX และ TAXII และมาตรฐานการขนส่งที่เป็นปัจจุบันเข้ากับโครงการป้องกันภัยคุกคามทางไซเบอร์ของสถานประกอบการทางนิวเคลียร์

....

๒.๓ ประโยชน์ที่ได้รับต่อตนเอง

☒ ต่อตนเอง .....ได้รับรู้ถึงวิธีการ ผลกระทบ การป้องกัน และการรับมือภัยคุกคามไซเบอร์ เพื่อใช้เป็นแนวทางในการปรับปรุงระบบเครือข่ายคอมพิวเตอร์ของสำนักงานปรมาณูเพื่อสันติที่อยู่ในความรับผิดชอบให้มีความมั่นคงปลอดภัยยิ่งขึ้น.....

.....

☒ ต่อหน่วยงาน .....ปัญหาภัยคุกคามไซเบอร์สามารถส่งผลกระทบต่อระบบความมั่นคงปลอดภัยของสถานประกอบการทางนิวเคลียร์ และระบบอื่น ๆ เช่น ระบบควบคุมเตาปฏิกรณ์นิวเคลียร์วิจัย เป็นต้น ทำให้หน่วยงานได้ตระหนักเกี่ยวกับความจำเป็นในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และระบบที่เกี่ยวข้องกับเทคโนโลยีนิวเคลียร์ รวมถึงความรู้เกี่ยวกับแนวปฏิบัติที่ดีในการซักซ้อมความมั่นคงทางคอมพิวเตอร์ที่สามารถนำไปปรับใช้ได้ในองค์กร.....

☐ อื่น ๆ(ระบุ) .....

ส่วนที่ ๓ ปัญหา/ อุปสรรค

.....**เนื้อหาของหลักสูตรเป็นไปตามที่กำหนด** .....

.....

ส่วนที่ ๔ ข้อคิดเห็นและข้อเสนอแนะ

.....การผลักดันให้เกิดการปรับปรุงเปลี่ยนแปลงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่จำเป็นสำหรับทุกหน่วยงาน เนื่องจากมีผลกระทบต่อภารกิจและความเชื่อมั่นของหน่วยงาน ซึ่งอาจรวมถึงอันตรายต่อชีวิต และทรัพย์สิน และความมั่นคงของประเทศ ดังนั้น หน่วยงานจึงจำเป็นต้องมีการปรับปรุงเปลี่ยนแปลงเพื่อเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงจัดทำมาตรฐานด้านความปลอดภัยทางนิวเคลียร์ที่ครอบคลุมถึงมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ และจัดให้มีการซักซ้อมการจำลองสถานการณ์ฉุกเฉินทางนิวเคลียร์และไซเบอร์เป็นประจำอยู่เสมอ.....

.....

(ลงชื่อ).....

(นายกฤษฎา ถิ่นทับปุด)

วันที่.....๑ ตุลาคม ๒๕๖๑.....

แบบ ICOP1

ส่วนที่ ๕ ความคิดเห็นของผู้บังคับบัญชา

.....

เห็นชอบต่อข้อคิดเห็น/ข้อเสนอแนะ

.....

.....

.....

(ลงชื่อ).....

(นางสุชิน อุดมสมพร)

ตำแหน่ง.....ผกยผ.....

วันที่ ๒๐ พ.ย. ๖๗

แบบICOP2

แผนงานการนำความรู้จากการประชุม/อบรม ไปใช้ประโยชน์

โดย .....นายกฤษฎา ถิ่นทับปุด.....

หน่วยงาน ....กองยุทธศาสตร์และแผนงาน สำนักงานปรมาณูเพื่อสันติ.....

ชื่อเรื่อง/หลักสูตร

(ภาษาไทย) .....

(ภาษาอังกฤษ)..Technical Meeting on Conducting Computer Security Exercises for Nuclear Security...

สถานที่ (หน่วยงาน/ประเทศ).....IAEA / สาธารณรัฐออสเตรีย.....

องค์ความรู้ที่นำมาใช้

๑. ความรู้ด้านเทคโนโลยีสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์

๒. ความรู้ด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๓. มาตรฐานและแนวปฏิบัติสำหรับการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ

แผนการใช้ประโยชน์

หัวข้อการนำความรู้ไปใช้	หน่วยงานที่เกี่ยวข้อง	งบประมาณที่คาดว่าจะใช้	ระยะเวลาดำเนินงาน	ผลลัพธ์/ผลสำเร็จของงาน
แผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และแผนบริหารความต่อเนื่อง (BCP)	กทส.กยผ.	๑,๐๐๐,๐๐๐ บาท	๑๒๐ วัน	ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของ สำนักงานปรมาณูเพื่อสันติ มีความมั่นคงปลอดภัยยิ่งขึ้น
การสร้างความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์	กทส. กยผ.			บุคลากรของสำนักงานปรมาณูเพื่อสันติมีความตระหนักเกี่ยวกับความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์
การสำรองและกู้คืนข้อมูลสารสนเทศ	กทส. กยผ.	๕๐๐,๐๐๐ บาท	๑๘๐ วัน	ระบบเทคโนโลยีสารสนเทศและฐานข้อมูลดิจิทัลที่สามารถให้บริการได้อย่างต่อเนื่อง
ปรับปรุงระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	กทส. กยผ.	๕,๐๐๐,๐๐๐ บาท	๑๘๐ วัน	ระบบเครือข่ายคอมพิวเตอร์ที่มีความมั่นคงปลอดภัย และสามารถให้บริการได้อย่างต่อเนื่อง มีประสิทธิภาพ

ลงชื่อ.....

(นายกฤษฎา ถิ่นทับปุด)

วันที่.....๑ ตุลาคม ๒๕๖๑...

ลงชื่อ.....

(.....)

ผู้บังคับบัญชา