แผนปฏิบัติการ
ด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ 1 (พ.ศ. 2563-2565)

สำนักงานสภาความมั่นคงแห่งชาติ
สำนักนายกรัฐมนตรี

แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

สำนักงานสภาความมั่นคงแห่งชาติ
สำนักนายกรัฐมนตรี

คำนำ

ยุทธศาสตร์ชาติด้านความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ให้ความสำคัญกับการป้องกันและแก้ไขปัญหาความมั่นคงแบบองค์รวม และให้หน่วยงานด้านความมั่นคงสามารถบูรณาการการทำงานให้เป็นไปในทิศทางเดียวกันอย่างมีประสิทธิภาพ โดยมีฐานข้อมูลด้านความมั่นคงที่ครอบคลุมทุกมิติ จึงได้กำหนดแผนการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวมและแนวทางการพัฒนาการบูรณาการข้อมูลด้านความมั่นคง ซึ่งจะเป็นกลไกสำคัญในการบูรณาการปฏิบัติงานของทุกหน่วยงานเป็นเอกภาพเดียวกัน

สำนักงานสภาความมั่นคงแห่งชาติในฐานะหน่วยงานรับผิดชอบหลักในการขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคงเห็นถึงความสำคัญของการมีฐานข้อมูลด้านความมั่นคงที่บูรณาการกันอย่างครบถ้วน อันจะเป็นประโยชน์ต่อหน่วยงานของรัฐและทุกภาคส่วนให้สามารถประสานการทำงานได้สอดคล้องกัน จึงได้จัดทำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) ซึ่งแผนปฏิบัติการดังกล่าวได้รับอนุมัติจากนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ แล้ว เมื่อวันที่ ๒๗ ธันวาคม ๒๕๖๒ โดยแผนปฏิบัติการฯ ฉบับนี้มุ่งเน้นการพัฒนา ๒ เป้าหมายหลักคือการมีระบบฐานข้อมูลและข้อมูลด้านความมั่นคงเพื่อสนับสนุนการแก้ปัญหาความมั่นคงระดับชาติ เพื่อให้หน่วยงานที่เกี่ยวข้องใช้เป็นแนวทางดำเนินการเชื่อมโยงข้อมูลด้านความมั่นคงผ่านระบบฐานข้อมูลด้านความมั่นคงระหว่างกันที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอต่อการสนับสนุนกลไกการตัดสินใจในการแก้ไขปัญหาความมั่นคงในระดับชาติอย่างมีประสิทธิภาพ

สำนักงานฯ หวังเป็นอย่างยิ่งว่าหน่วยงานที่เกี่ยวข้องจะร่วมขับเคลื่อนแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) เพื่อเป็นแนวทางและกลไกในการกำหนดแผนงาน/โครงการ และงบประมาณของหน่วยงาน และบูรณาการการทำงานร่วมกันให้สำเร็จตามเป้าหมายในระยะแรก ให้บังเกิดผลสัมฤทธิ์ต่อไป

พลเอก
(สมศักดิ์ รุ่งสิตา)
เลขาธิการสภาความมั่นคงแห่งชาติ

สารบัญ
แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

ส่วนที่ ๑ บทสรุปผู้บริหาร

ด้วย ยุทธศาสตร์ชาติด้านความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ให้ความสำคัญกับ “ประเทศชาติมั่นคง ประชาชนมีความสุข” จึงกำหนดให้มีแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ซึ่งให้ความสำคัญกับการกำหนดแผนย่อยการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม เพื่อเสริมสร้างกลไกการแก้ไขปัญหา ตลอดจนขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคงแบบองค์รวมให้เป็นรูปธรรมพร้อมตอบสนองต่อปัญหาในทุกมิติ พร้อมทั้งกำหนดแนวทางการพัฒนาที่เกี่ยวกับการบูรณาการข้อมูลด้านความมั่นคงไว้อย่างชัดเจน เนื่องจากการบริหารจัดการข้อมูลด้านความมั่นคงที่ผ่านมามีความซ้ำซ้อนและมีอุปสรรคในด้านต่าง ๆ เช่น ด้านกฎหมาย กฎ ระเบียบ ด้านนโยบายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานเป็นไปด้วยความล่าช้าและขาดหน่วยงานกลางดำเนินการที่ชัดเจน ด้านเทคโนโลยีสารสนเทศในการบูรณาการฐานข้อมูลและการเชื่อมโยงแลกเปลี่ยนข้อมูล และด้านบุคลากรในการบริหารจัดการข้อมูล ทำให้รัฐบาลเห็นความสำคัญของการบูรณาการฐานข้อมูลเพื่อแก้ไขปัญหาดังกล่าว

ดังนั้น สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) เพื่อสนับสนุนการวางระบบบูรณาการข้อมูลด้านความมั่นคงให้มีประสิทธิภาพและสนับสนุนการแก้ไขปัญหาความมั่นคงได้ทุกมิติและทุกรูปแบบตามที่ยุทธศาสตร์ชาติด้านความมั่นคงและแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ให้ความสำคัญ ทั้งนี้ **แผนปฏิบัติการฯ มีเป้าหมายเพื่อสร้างระบบฐานข้อมูลและข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอสามารถสนับสนุนกลไกการตัดสินใจเพื่อแก้ไขปัญหาความมั่นคงในระดับชาติ** โดยมีวัตถุประสงค์เพื่อจัดทำฐานข้อมูลด้านความมั่นคง และพัฒนาระบบข้อมูลในการประเมินสถานการณ์ในการรับมือภัยคุกคาม ตลอดจนเพิ่มประสิทธิภาพการแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงาน ด้านความมั่นคง และบริหารจัดการข้อมูลด้านความมั่นคงที่ทันสมัย โดยกำหนดแนวทางการพัฒนา ๔ แนวทาง ดังนี้

แนวทางการพัฒนาที่ ๑ นโยบายการบูรณาการฐานข้อมูลด้านความมั่นคง มุ่งเน้นการศึกษา ทบทวน ปรับปรุง นโยบาย แผน กฎ ระเบียบ เพื่อกำหนดกรอบแนวทางดำเนินงานของหน่วยงานที่เกี่ยวข้องกับฐานข้อมูลด้านความมั่นคง รวมทั้งเสริมสร้างและบูรณาการข้อมูลร่วมกันเพื่อสนับสนุนยุทธศาสตร์ชาติด้านความมั่นคง

แนวทางการพัฒนาที่ ๒ การพัฒนาระบบฐานข้อมูลด้านความมั่นคง มุ่งเน้นพัฒนาระบบฐานข้อมูลด้านความมั่นคงที่เหมาะสม โดยส่งเสริมการจัดทำประเภทบัญชีข้อมูลด้านความมั่นคง พัฒนาระบบเทคโนโลยีที่ทันสมัยให้กับหน่วยงานที่มีหน้าที่ดำเนินการในกิจการงานความมั่นคง รวมทั้งพัฒนาและวางแผนระบบโครงสร้างอัตรากำลัง และศักยภาพของบุคลากรให้มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้าน

แนวทางการพัฒนาที่ ๓ การดำเนินงานด้านเทคนิคเพื่อบูรณาการข้อมูลระหว่างหน่วยงาน ให้ความสำคัญกับการจัดทำ Big Data Platform ด้านความมั่นคง โดยพัฒนาโครงสร้างพื้นฐานการจัดเก็บและประมวลผลหน่วยงานที่เกี่ยวข้องที่เหมาะสม พัฒนาระบบสารสนเทศเพื่อบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูล

สำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และพัฒนาระบบรายการข้อมูลภาครัฐ (Government Data Catalog)

แนวทางการพัฒนาที่ ๔ การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง กำหนดแนวทางขับเคลื่อนแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) ที่สอดคล้องกับ “แนวความคิดการบริหารจัดการยุทธศาสตร์ชาติด้านความมั่นคง” ให้ความสำคัญกับการบริหารจัดการแผนปฏิบัติการฯ ให้สอดคล้องกับประเด็นการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวมภายใต้ยุทธศาสตร์ชาติด้านความมั่นคง และสร้างกลไกความร่วมมือ/ความตกลงหรือการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงานตลอดจนเสริมสร้างและพัฒนาองค์ความรู้เกี่ยวกับการมีข้อมูลและการบูรณาการ

(๑) **ระดับนโยบาย** การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคงในระดับนโยบาย มอบให้ **สภาความมั่นคงแห่งชาติ** (โดย สำนักงานสภาความมั่นคงแห่งชาติ : สมช.) เป็นหน่วยรับผิดชอบ โดยแต่งตั้งคณะกรรมการบูรณาการฐานข้อมูลด้านความมั่นคง โดยมีรองนายกรัฐมนตรีที่นายกรัฐมนตรีมอบหมายเป็นประธาน เพื่อทำหน้าที่กำหนดนโยบายและแนวทางการบูรณาการฐานข้อมูลด้านความมั่นคง

(๒) **ระดับอำนวยการ** การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในระดับอำนวยการและประสานการปฏิบัติ มอบให้ **กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร** (กอ.รมน.) เป็นหน่วยงานกลางรับผิดชอบทำหน้าที่เป็นศูนย์กลางข้อมูลด้านความมั่นคง (Data Center) เชื่อมโยงและประสานกับหน่วยงานด้านความมั่นคงอื่น ๆ

(๓) **ระดับปฏิบัติ หน่วยงานระดับกระทรวง/กรมที่เกี่ยวข้อง**กับแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง รวมทั้งศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) เป็นหน่วยดำเนินการ

ทั้งนี้ การบูรณาการข้อมูลด้านความมั่นคงระหว่างหน่วยงานด้านความมั่นคงและหน่วยงานที่มีภารกิจสนับสนุนงานด้านความมั่นคงภายใต้แผนปฏิบัติการฯ จะถูกจัดอยู่ในบัญชีข้อมูลด้านความมั่นคงที่ดำเนินการทั้งหมด ๑๐ ด้านสำคัญ ได้แก่ ๑) ฐานข้อมูลความมั่นคงด้านการเตรียมพร้อมแห่งชาติ ๒) ฐานข้อมูลความมั่นคงด้านการบริหารจัดการชายแดน ๓) ฐานข้อมูลด้านการรักษาผลประโยชน์ของชาติทางทะเล ๔) ฐานข้อมูลความมั่นคงด้านอาชญากรรมข้ามชาติและการก่อการร้าย ๕) ฐานข้อมูลความมั่นคงด้านปัญหาผู้หลบหนีเข้าเมือง ๖) ฐานข้อมูลความมั่นคงด้านอัตลักษณ์บุคคล ๗) ฐานข้อมูลความมั่นคงด้านการแก้ไขปัญหาพื้นที่สามจังหวัดชายแดนภาคใต้ ๘) ฐานข้อมูลความมั่นคงด้านการข่าว ๙) ฐานข้อมูลความมั่นคงด้านการป้องกันและปราบปรามการค้ามนุษย์ และ ๑๐) ฐานข้อมูลความมั่นคงอื่น ๆ เพื่อให้การจัดทำฐานข้อมูลด้านความมั่นคง การทำบัญชีข้อมูลด้านความมั่นคง และการเชื่อมโยงข้อมูลด้านความมั่นคงมีความสอดคล้องซึ่งกันและกัน สามารถนำไปใช้ในการป้องกันและแก้ไขปัญหาความมั่นคงได้อย่างมีประสิทธิภาพ รวมทั้งใช้เป็นข้อมูลประกอบการตกลงใจของหน่วยงานทั้งในระดับนโยบาย ระดับอำนวยการ และระดับปฏิบัติได้อย่างครอบคลุม

ส่วนที่ ๒ ความสอดคล้องกับแผน ๓ ระดับ ตามมติคณะรัฐมนตรี เมื่อวันที่ ๔ ธันวาคม ๒๕๖๐

๒.๑ ยุทธศาสตร์ชาติ (แผนระดับที่ ๑)

ยุทธศาสตร์ชาติด้านความมั่นคง

(๑) เป้าหมาย

การบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมีประสิทธิภาพ

(๒) ประเด็นยุทธศาสตร์

ข้อที่ ๔.๕ การพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม เพื่อให้กลไกสำคัญต่าง ๆ ทำงานได้อย่างมีประสิทธิภาพ สามารถส่งเสริมและสนับสนุนการบริหารและพัฒนาประเทศได้อย่างแท้จริง เป็นรูปธรรม มีการใช้หลักธรรมาภิบาล และการบังคับใช้กฎหมายอย่างเคร่งครัดและมีประสิทธิภาพ สามารถขจัดปัญหาการทุจริตและประพฤติมิชอบอย่างจริงจัง เกิดความมั่นใจได้ว่าหน่วยงานรับผิดชอบทั้งหลักและรองพร้อมรับมือ กับภัยคุกคามทุกรูปแบบทั้งในปัจจุบันและอนาคต

๒.๒ แผนระดับที่ ๒

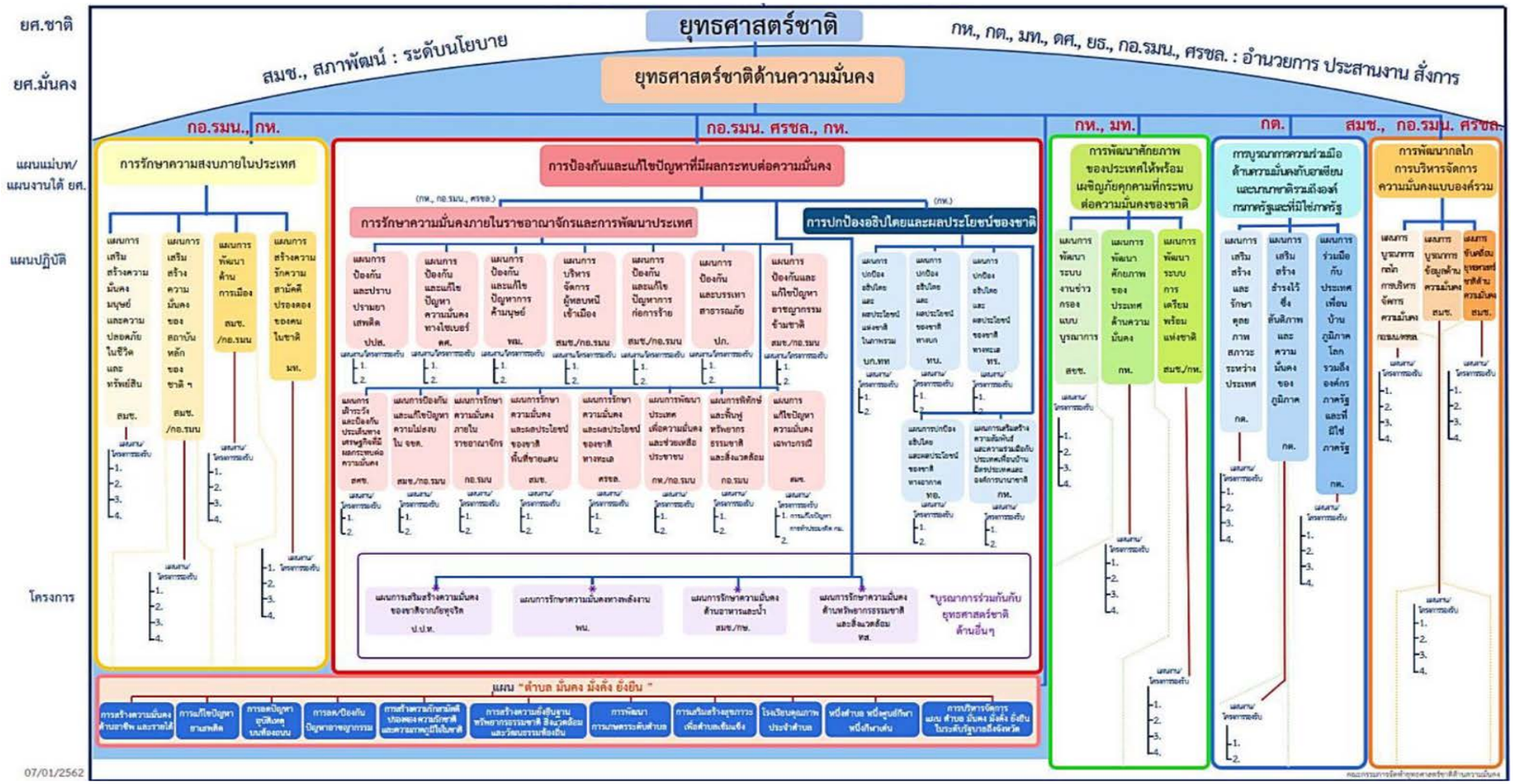
๒.๒.๑ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง

๑) แผนย่อย : การพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม

๒) แนวทางการพัฒนา : บูรณาการข้อมูลด้านความมั่นคง มุ่งพัฒนาส่งเสริมการวางแผนคู่ขนานแบบบูรณาการให้สอดคล้องรองรับยุทธศาสตร์ชาติในทุก ๆ ด้าน รวมไปถึงการบริหารประเทศที่เกี่ยวข้องในทุกมิติอย่างครบถ้วนสมบูรณ์และมีประสิทธิภาพ เสริมสร้างผลักดันการบริหารจัดการตลอดถึงการบูรณาการการดำเนินการในทุกด้าน ให้ประสานสอดคล้องและสามารถปฏิบัติร่วมกันได้อย่างใกล้ชิดระหว่างหน่วยงานด้านความมั่นคง ด้านเศรษฐกิจ และด้านอื่น ๆ ที่เกี่ยวข้อง พร้อมทั้งครอบคลุมการสร้างความมั่นคงให้กับประเทศชาติในทุกมิติอย่างยั่งยืน โดยการวางระบบการบูรณาการข้อมูลด้านความมั่นคงให้มีประสิทธิภาพสามารถสนับสนุนการวางแผนและแก้ไขปัญหาความมั่นคงได้ทุกมิติทุกรูปแบบ โดยจัดทำแผนย่อยการบูรณาการข้อมูลด้านความมั่นคงขึ้นรองรับพร้อมทั้งกำหนดแผนงาน/โครงการสำคัญไว้อย่างชัดเจนด้วย โดยมีแนวคิดในการดำเนินการที่สำคัญ ได้แก่ (๑) การวางแผนคู่ขนานกันทั้งทางดิ่งและทางระดับ เพื่อให้แผนทุกระดับเสร็จสมบูรณ์ในเวลาไล่เลี่ยกัน สามารถปฏิบัติได้อย่างรวดเร็ว (๒) การทำงานแบบบูรณาการร่วมกันตั้งแต่ขั้นการวางแผนการปฏิบัติและการประเมินผล เพื่อให้เกิดประสิทธิภาพสูงสุด และ (๓) การบริหารจัดการข้อมูลด้านความมั่นคงแบบบูรณาการร่วมกัน เพื่อให้มีข้อมูลที่ทันสมัย ถูกต้องและสมบูรณ์เพียง

๓) เป้าหมายของแผนย่อย : กลไกการบริหารจัดการความมั่นคงมีประสิทธิภาพสูงขึ้น

๔) ตัวชี้วัด : ระดับประสิทธิภาพการดำเนินงานของหน่วยงานด้านการจัดการความมั่นคง



ภาพที่ ๑ แนวความคิดการบริหารจัดการยุทธศาสตร์ชาติด้านความมั่นคง

๒.๒.๒ แผนการปฏิรูปประเทศด้านการบริหารราชการแผ่นดิน

๑) เรื่องและประเด็นการปฏิรูปที่ ๒ ระบบข้อมูลภาครัฐมีมาตรฐาน ทันสมัย และเชื่อมโยงกัน ก้าวสู่รัฐบาลดิจิทัล

๒) กลยุทธ์

(๑) บูรณาการและยกระดับโครงสร้างพื้นฐานรัฐบาลดิจิทัล

(๒) นำระบบดิจิทัลมาใช้ในการปฏิบัติงาน และการบริหารราชการ

(๓) บูรณาการข้อมูลของหน่วยงานภาครัฐเพื่อการบริหารราชการแผ่นดิน

๒.๒.๓ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ส่วนที่ ๔ ยุทธศาสตร์การพัฒนาประเทศ

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

แนวทางการพัฒนาหลักที่ ๓.๒ การพัฒนาเสริมสร้างศักยภาพการป้องกันประเทศเพื่อเตรียมความพร้อมในการรับมือภัยคุกคามทั้งการทหารและภัยคุกคามอื่น ๆ

แนวทางการพัฒนาย่อยที่ ๓.๒.๒ พัฒนาระบบงานด้านการข่าวที่มีประสิทธิภาพ มีกลไกเสริมสร้างความร่วมมือพัฒนาองค์ความรู้ ศึกษาวิเคราะห์แนวโน้มภัยคุกคาม รวมทั้งจัดทำฐานข้อมูลด้านการข่าวที่มีความเชื่อมโยงระหว่างหน่วยงานภายในประเทศและต่างประเทศอย่างเป็นระบบ ให้มีความพร้อมในการสนับสนุนข้อมูลเพื่อเตรียมการรับมือภัยคุกคามด้านความมั่นคงทั้งในประเทศและในระดับนานาชาติ

๒.๒.๔ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

ส่วนที่ ๔ การขับเคลื่อนนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

ภาพรวมของการขับเคลื่อนนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ - ๒๕๖๕) เป็นกรอบทิศทางหลักที่ทุกส่วนราชการที่เกี่ยวข้องนำไปกำหนดหรือบูรณาการให้สอดคล้องกับนโยบาย/แผนยุทธศาสตร์ของกระทรวง/กรม รวมถึงการกำหนดนโยบาย/ยุทธศาสตร์เฉพาะเรื่อง/แนวทาง/มาตรการ กรณีที่มีความสำคัญรองรับการดำเนินการตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ ตลอดจนการจัดทำแผนงานโครงการรองรับ โดยสภาความมั่นคงแห่งชาติซึ่งมีนายกรัฐมนตรีเป็นประธานเป็นกลไกหลักในการอำนวยการและขับเคลื่อนในระดับชาติ คณะกรรมการภายใต้สภาความมั่นคงแห่งชาติเป็นกลไกสนับสนุนในการกำกับติดตาม บูรณาการและขับเคลื่อนเชิงนโยบาย และสำนักงานสภาความมั่นคงแห่งชาติรับผิดชอบภาพรวมในการอำนวยการ กำกับ ติดตามและขับเคลื่อนนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติให้ประสานสอดคล้องกัน โดยมีการประเมินสถานการณ์และประเมินผลการดำเนินการ ทั้งนี้ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) และศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) ทำหน้าที่ร่วมประสานการปฏิบัติตามนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ ซึ่งแนวทางการขับเคลื่อนดังกล่าวจะสอดรับและเป็นไปในแนวทางการดำเนินขับเคลื่อนแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคงด้วย

๒.๒.๕ นโยบายรัฐบาล (นโยบายของคณะรัฐมนตรีที่แถลงต่อรัฐสภา เมื่อวันที่ ๒๕ กรกฎาคม ๒๕๖๒)

นโยบายหลักด้านการปฏิรูปการบริหารจัดการภาครัฐ เพื่อให้การขับเคลื่อนการพัฒนาประเทศสามารถบริหารจัดการได้อย่างมีประสิทธิภาพมากขึ้น การปฏิรูประบบการบริหารจัดการภาครัฐ โดยการนำเทคโนโลยีดิจิทัลเข้ามาช่วยในการให้บริการของภาครัฐ และการบูรณาการการทำงานของหน่วยงานต่าง ๆ เช่น **การพัฒนาระบบข้อมูลขนาดใหญ่ในการบริหารราชการแผ่นดิน**ที่มีระบบการวิเคราะห์ แบ่งปันข้อมูลที่มีประสิทธิภาพ และเชื่อถือได้ **และการเปิดเผยข้อมูลภาครัฐสู่สาธารณะ** โดยหน่วยงานของรัฐในทุกระดับต้องเปิดเผยและเชื่อมโยงข้อมูลซึ่งกันและกัน ทั้งในระหว่างหน่วยงานของรัฐด้วยกันเอง และระหว่างหน่วยงานรัฐกับประชาชน เพื่อให้ทุกภาคส่วนมีความเข้าใจถึงสถานการณ์ และแนวทางการแก้ไขปัญหาต่าง ๆ ของประเทศที่มีความซับซ้อน ปรับเปลี่ยนให้เป็นการทำงานเชิงรุก เน้นการยกระดับไปสู่ความร่วมมือกันของทุกภาคส่วนอย่างจริงจัง แสวงหาความคิดริเริ่มและสร้างนวัตกรรม โดยมีการคาดการณ์สถานการณ์ วิเคราะห์ความเสี่ยง และผลกระทบที่คาดว่าจะเกิดขึ้นไว้ล่วงหน้า เพื่อให้สามารถเตรียมความพร้อมรองรับการเปลี่ยนแปลงอย่างฉับพลันในด้านต่าง ๆ ได้อย่างมีประสิทธิภาพ

ส่วนที่ ๓ สาระสำคัญของแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๑ การประเมินสถานการณ์ ปัญหา และความจำเป็นของแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง

การจัดทำฐานข้อมูลด้านความมั่นคงมีความสำคัญเนื่องจากหน่วยงานด้านความมั่นคงในปัจจุบันมีการจัดเก็บข้อมูลต่าง ๆ ในฐานข้อมูลของหน่วยงานโดยรัฐบาลได้กำหนดแนวทางในการรวบรวมข้อมูลของราชการในภาคส่วนต่าง ๆ ประกอบกับการดำเนินงานที่ผ่านมาการรวบรวมข้อมูลหรือเชื่อมโยงข้อมูลระหว่างหน่วยงานเป็นเรื่องที่ทำได้ยาก ทำให้การแลกเปลี่ยนและประสานข้อมูลระหว่างหน่วยงานมีปัญหาและอุปสรรค เช่น ข้อมูลอาชญากรรมของตำรวจกับข้อมูลลายนิ้วมือของสถาบันนิติวิทยาศาสตร์ เป็นต้น อย่างไรก็ตาม ในปัจจุบันการเชื่อมโยงข้อมูลสามารถทำได้สะดวกขึ้น เนื่องจากมีการจัดเก็บข้อมูลในพื้นที่ไซเบอร์ ซึ่งในพื้นที่ไซเบอร์หน่วยงานต่าง ๆ สามารถเข้าไปเชื่อมโยงหรือใช้ข้อมูลในพื้นที่ (Platform) การจัดเก็บข้อมูลได้เพื่อใช้ประโยชน์ในงานต่าง ๆ ได้อย่างทันท่วงที

การดำเนินงานของหน่วยงานด้านความมั่นคงที่ผ่านมาเกี่ยวกับฐานข้อมูลด้านความมั่นคง ได้แก่ **๑) กระทรวงมหาดไทย** ดำเนินการ (๑) ระบบการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (LINKAGE CENTER) (๒) ระบบการเชื่อมโยงข้อมูลทะเบียนประวัติราษฎร (IKNO) (๓) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือ (Automated fingerprint identification systems: AFIS) และ (๔) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยภาพใบหน้า (Face Recognition) **๒) กระทรวงกลาโหม** ดำเนินการ (๑) โครงการพัฒนาระบบสารสนเทศเพื่อการระดมสรรพกำลัง และ (๒) โครงการพัฒนาระบบสารสนเทศเพื่อการกำลังสำรองและการสัสดี **๓) กระทรวงยุติธรรม** ดำเนินการ (๑) ระบบฐานข้อมูลดีเอ็นเอ (๒) ระบบฐานข้อมูลลายพิมพ์นิ้วมือ (๓) ระบบฐานข้อมูลบุคคลสูญหายและศพนิรนาม และ (๔) ระบบฐานข้อมูลการตรวจพิสูจน์ทางนิติวิทยาศาสตร์ **๔) สำนักงานตำรวจแห่งชาติ** โดย (๑) สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (ระบบการสืบค้นข้อมูลหมายจับ) (๒) ตำรวจภูธรภาค ๙ และ (๓) สำนักงานตรวจคนเข้าเมือง (ข้อมูลแรงงานต่างด้าว ๓ สัญชาติ (เมียนมา ลาว กัมพูชา)) **และ ๕) ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.)** ดำเนินงานเกี่ยวข้องกับการรักษาผลประโยชน์ของชาติทาง

ทะเลต่อจากศูนย์ประสานการปฏิบัติในการรักษาผลประโยชน์ของชาติทางทะเลภายใต้พระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ. ๒๕๖๒ มีภารกิจ หน้าที่เกี่ยวข้องในการรักษาผลประโยชน์ของชาติทางทะเล รวมถึงการบูรณาการข้อมูลของหน่วยงานของรัฐให้สามารถติดต่อ เชื่อมโยง หรือแลกเปลี่ยนข้อมูลระหว่างกันได้ เพื่อประโยชน์ในการรักษาผลประโยชน์ของชาติทางทะเลหรือกิจกรรมทางทะเล

นอกจากนี้ การบูรณาการฐานข้อมูลด้านความมั่นคงร่วมกับหน่วยงานที่เกี่ยวข้องโดยแต่งตั้งคณะอนุกรรมการ ๓ คณะ ได้แก่ **๑) คณะอนุกรรมการจัดทำฐานข้อมูลด้านความมั่นคงในการแก้ไขปัญหาจังหวัดชายแดนภาคใต้** กำกับดูแลโครงการใน ๒ ระดับ ได้แก่ (๑) ระดับยุทธศาสตร์ โดยสำนักงานสภาความมั่นคงแห่งชาติ ดำเนินโครงการเพิ่มประสิทธิภาพการบูรณาการฐานข้อมูลด้านความมั่นคงจังหวัดชายแดนภาคใต้ (ตามมติคณะกรรมการขับเคลื่อนการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ ครั้งที่ ๒/๒๕๖๑ เมื่อวันที่ ๑๙ เมษายน ๒๕๖๑) และ (๒) ระดับยุทธการและยุทธวิธี โดยกองอำนวยการรักษาความมั่นคงภายในภาค ๔ ส่วนหน้า และกองทัพอากาศดำเนินโครงการบูรณาการจัดทำฐานข้อมูลกลางด้านความมั่นคงจังหวัดชายแดนภาคใต้และโครงการถ่ายภาพถ่ายทางอากาศพื้นที่จังหวัดชายแดนภาคใต้ **๒) คณะอนุกรรมการเฉพาะกิจพิจารณาแนวทางการจัดตั้งฐานข้อมูลอัตลักษณ์บุคคลแห่งชาติ** ดำเนินโครงการพัฒนาระบบการเชื่อมโยงข้อมูลอัตลักษณ์บุคคลเพื่อจัดตั้งฐานข้อมูลอัตลักษณ์บุคคลแห่งชาติให้มีความชัดเจน เหมาะสม และเกิดประสิทธิภาพสูงสุด **และ ๓) คณะอนุกรรมการพิจารณาแนวทางการจัดทำฐานข้อมูลด้านความมั่นคง** มีอำนาจหน้าที่คือ (๑) ปรับปรุงร่างคำสั่งแต่งตั้งคณะทำงานจัดทำร่างแผนฐานข้อมูลด้านความมั่นคง โดยมีผู้แทนหน่วยงานที่เกี่ยวข้องที่รับผิดชอบด้านนโยบายและเทคนิค และ (๒) ให้จัดทำร่าง Platform ฐานข้อมูลด้านความมั่นคง เพื่อรองรับการจัดทำฐานข้อมูลด้านความมั่นคง และเสนอคณะทำงานฯ/คณะอนุกรรมการฯ

การจัดเก็บข้อมูลภาครัฐได้แบ่งพื้นที่การเก็บเพื่อให้เข้ากับความสำคัญของข้อมูลต่าง ๆ ที่จะต้องเชื่อมโยงหรือบูรณาการกับหน่วยงานต่าง ๆ ออกเป็น ๓ กลุ่ม ได้แก่ ๑) พื้นที่เก็บข้อมูลของรัฐบาล (Government Cloud) ที่จะใช้เป็นพื้นที่เก็บข้อมูลขนาดใหญ่ที่มีการเชื่อมโยงกันในหน่วยงานภาครัฐทั้งหมด ๒) พื้นที่เก็บข้อมูลของกระทรวง (Ministry Cloud) เป็นพื้นที่เก็บข้อมูลสำคัญที่จะรวมในแต่ละกระทรวง และ ๓) พื้นที่เก็บข้อมูลของหน่วยงานย่อย (Agency Cloud) จะเป็นพื้นที่เก็บข้อมูลสำคัญที่รวมกันในแต่ละกรม กอง หรือสำนักโดยโครงสร้างของพื้นที่เก็บข้อมูลนี้เป็นการเริ่มต้นสำหรับการจัดทำพื้นที่เก็บข้อมูลของแต่ละหน่วยงาน ซึ่งจะมีผู้รับผิดชอบหลักคือ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ซึ่งหน่วยงานด้านความมั่นคงก็จะได้นำตัวแบบดังกล่าวมาปรับใช้ในการเชื่อมโยงข้อมูลด้านความมั่นคง เพื่อการทำงานที่รวดเร็วและสร้างความปลอดภัยให้กับประเทศได้อย่างมีประสิทธิภาพ

ดังนั้น เพื่อให้การจัดทำฐานข้อมูลและการบูรณาการข้อมูลด้านความมั่นคงเกิดการใช้ประโยชน์จากข้อมูลความมั่นคงแต่ละหน่วยงานในการตอบสนองการดำเนินงานด้านความมั่นคงของประเทศตามแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง สำนักงานสภาความมั่นคงแห่งชาติ จึงได้จัดทำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) เพื่อสนับสนุนการวางระบบบูรณาการข้อมูลด้านความมั่นคงให้มีประสิทธิภาพและสนับสนุนการแก้ไขปัญหาความมั่นคงทุกมิติ

๓.๑.๑ นิยามศัพท์

“ความมั่นคงแห่งชาติ”[๑] หมายความว่า ภาวะที่ประเทศปลอดจากภัยคุกคามต่อเอกราช อธิปไตย บูรณภาพแห่งอาณาเขต สถาบันศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน หรือที่กระทบต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข รวมทั้งความพร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบ

“ข้อมูลด้านความมั่นคง”[๒] หมายความว่า ข้อมูลที่เกี่ยวข้องกับความมั่นคงของประเทศ ควรได้รับการปกป้องด้วยมาตรการความปลอดภัยขั้นสูงสุด มีการเข้ารหัส และจำกัดสิทธิ์การเข้าถึงอย่างเข้มงวด เนื่องจากการรั่วไหลของข้อมูลจะสร้างความเสียหายต่อประเทศเป็นอย่างมาก

“ระบบฐานข้อมูลด้านความมั่นคง” หมายความว่า ระบบการจัดการข้อมูลด้านความมั่นคง ระหว่างผู้ใช้งานกับข้อมูลอิเล็กทรอนิค และการสร้างกระบวนการร้องขอของผู้ใช้งานอันแสดงถึงการกระทำกับข้อมูลที่อยู่ในฐานข้อมูล

๓.๑.๒ สภาพปัญหาและบริบทการจัดทำฐานข้อมูลด้านความมั่นคง

๑) ด้านกฎหมาย กฎ ระเบียบ

ปัญหาและอุปสรรคของกฎหมายเกี่ยวกับการเชื่อมโยงข้อมูลภาครัฐ ประกอบด้วย ๒ ประการสำคัญ ได้แก่ (๑) **ข้อมูลที่เกี่ยวข้องกับกฎหมายมีอยู่ ๓ ลักษณะ** กล่าวคือ ข้อมูลสาธารณะและข้อมูลข่าวสารของทางราชการ ข้อมูลส่วนบุคคลและข้อมูลความมั่นคงหรือข้อมูลความลับที่มีกฎหมายหรือกฎระเบียบห้ามเปิดเผย และข้อมูลที่มีกฎหมายห้ามเปิดเผยข้อมูล และ (๒) **ปัญหาในทางปฏิบัติ** ได้แก่ เจ้าหน้าที่ของรัฐปฏิเสธการเข้าถึงการเปิดเผยข้อมูล หรือการเชื่อมโยงข้อมูล เพราะขาดความเข้าใจในการแยกประเภทข้อมูล หรือถือปฏิบัติตามระเบียบของหน่วยงานที่ต้องมีคำขอหรือได้รับอนุมัติก่อนจึงจะให้ข้อมูลได้

อย่างไรก็ตาม ปัจจุบันพระราชบัญญัติการบริหารงานและการใช้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ซึ่งมีผลบังคับใช้เมื่อวันที่ ๒๓ พฤษภาคม ๒๕๖๒ ทำให้การเชื่อมโยงระหว่างหน่วยงานภาครัฐในระยะต่อไปเปิดกว้างมากขึ้น อาทิ มาตรา ๑๒ (๑) การจัดทำข้อมูลในภารกิจให้อยู่ในรูปแบบข้อมูลดิจิทัล โดยสามารถแลกเปลี่ยนกับหน่วยงานของรัฐแห่งอื่นและนำไปประมวลผลต่อไปได้ มาตรา ๑๒ (๒) การจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัล ให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ และมาตรา ๑๓ ให้หน่วยงานของรัฐจัดให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลที่มีการจัดทำและครอบครองตามที่หน่วยงานของรัฐแห่งอื่นร้องขอที่จะเกิดการบูรณาการร่วมกัน เป็นต้น รวมทั้งมีธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) เป็นกรอบในการบริหารจัดการข้อมูล

---

[๑] มาตรา ๔ ของพระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๙

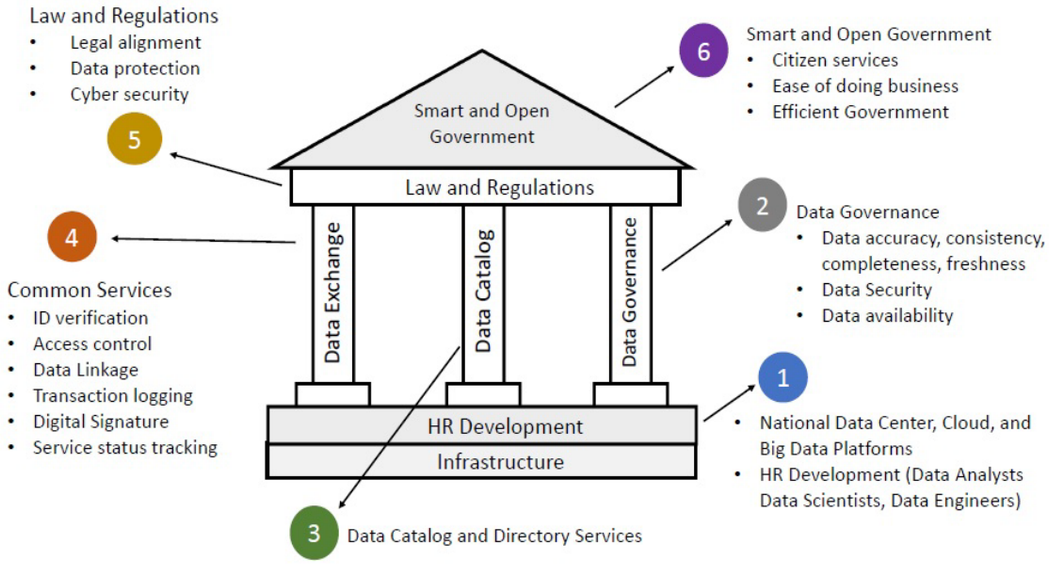
[๒] ร่างมาตรฐานและแนวทางปฏิบัติการออกแบบโครงสร้างพื้นฐานทางด้านสารสนเทศเพื่อการประมวลผลข้อมูลภาครัฐ โดยคณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๒) ด้านนโยบาย

หน่วยงานด้านความมั่นคงได้ให้ความสำคัญกับการจัดทำฐานข้อมูลเพื่อใช้ข้อมูลประเภทต่าง ๆ ในภารกิจของหน่วยงานถึงแม้จะมีความพยายามในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานแต่ยังคงเป็นไปด้วยความล่าช้าและขาดหน่วยงานกลางดำเนินการที่ชัดเจน โดยปัจจุบันขาดการกำหนด Platform การบูรณาการข้อมูลด้านความมั่นคงเพื่อเป็นตัวกลางอำนวยความสะดวกในการแลกเปลี่ยนและบูรณาการเชื่อมโยงข้อมูลในการดำเนินงานด้านความมั่นคง (Data Exchange Platform) ดังนั้น ควรมีการออกแบบพิมพ์เขียว (Blueprint) Platform การบูรณาการข้อมูลด้านความมั่นคง เพื่อสนองตอบต่อการกำหนดนโยบาย แผน และการปฏิบัติของหน่วยงานด้านความมั่นคงในการป้องกันและแก้ไขปัญหาที่กระทบต่อความมั่นคงของชาติ ประกอบกับบางหน่วยงานซึ่งเป็นเจ้าของหน่วยงานและแหล่งต้นทางของข้อมูล (Data Owner and Data Source) ยังขาดความพร้อมในการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน อาทิ การขาดการบริหารจัดการข้อมูลที่ดีจึงทำให้ข้อมูลที่จัดเก็บไม่มีคุณภาพและไม่ทันสมัย และการขาดกรอบสถาปัตยกรรมการบูรณาการข้อมูลจึงทำให้ไม่สามารถเชื่อมโยงข้อมูลได้อย่างมีประสิทธิภาพ

๓) ด้านเทคโนโลยีสารสนเทศ

กรอบการให้บริการข้อมูลภาครัฐ ประกอบด้วย ๖ ส่วน ที่จะสร้างให้เกิดระบบนิเวศข้อมูลที่สามารถถูกใช้ประโยชน์ร่วมกันได้อย่างเป็นระบบ ดังนี้



ภาพที่ ๒ แนวคิดของการให้บริการข้อมูลภาครัฐ (Government Data Service Framework)

๑. การพัฒนาโครงสร้างพื้นฐานการประมวลผลภาครัฐที่เหมาะสม มีประสิทธิผลในการใช้งานทั้งในมิติด้านความต่อเนื่องของบริการ การรักษาความปลอดภัย และการแลกเปลี่ยนเชื่อมโยงข้อมูลอย่างเป็นระบบ ซึ่งสถาปัตยกรรมโครงสร้างพื้นฐานควรเป็นแบบแบ่งปันที่ผู้รับบริการมองเสมือนว่าเป็นโครงสร้างเดียวที่ใช้ร่วมกัน ในขณะที่ทางกายภาพโครงสร้างพื้นฐานเป็นแบบกระจายที่มีการเช่าใช้คลาวด์ผสมกับการสร้างดาต้าเซนเตอร์

หน่วยงานภาครัฐสามารถวางแผนการปรับโครงสร้างพื้นฐานการประมวลผลที่เหมาะสมให้กับหน่วยงานได้ โดยทำการวิเคราะห์ช่องว่าง (Gap Analysis) ตามแนวทางที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดขึ้น

การวางแผนและดำเนินงานด้านการพัฒนาบุคลากรภาครัฐ เพื่อเตรียมความพร้อมสำหรับการประยุกต์ใช้ข้อมูลในการวิเคราะห์เพื่อวางแผนยุทธศาสตร์ การปฏิบัติงานของเจ้าหน้าที่ การบริหารงานของหน่วยงานภาครัฐ และการให้บริการประชาชน โดยเน้นการอบรมเพื่อพัฒนานักวิเคราะห์ข้อมูล นักวิทยาศาสตร์ข้อมูล และวิศวกรข้อมูลโดยอาศัยความร่วมมือกับเครือข่ายมหาวิทยาลัย และสำนักงานคณะกรรมการข้าราชการพลเรือน

๒. การส่งเสริมให้หน่วยงานภาครัฐสามารถกำกับดูแลข้อมูลของตนให้มีความถูกต้อง ตรงกัน สมบูรณ์ และทันสมัย รวมทั้งอยู่ในสภาพที่พร้อมใช้งานโดยมีการกำกับดูแลความปลอดภัยของข้อมูลให้ได้มาตรฐานตามชั้นความลับ เพื่อให้การใช้ประโยชน์และการบริการข้อมูลเกิดขึ้นได้อย่างเป็นรูปธรรม

๓. การพัฒนาระบบรายการข้อมูลภาครัฐ (Government Data Catalog) โดยรวบรวมรายละเอียดของข้อมูล (Metadata) สำคัญจากหน่วยงานภาครัฐทั้งหมดเพื่อจัดสร้างเป็นรายการจากนั้นพัฒนากลไกการสืบค้นในมิติต่าง ๆ เพื่อให้บริการการสืบค้นข้อมูล (Directory Service) โดยระบบรายการข้อมูลและหน้าจอสืบค้นที่ใช้งานง่ายจะเป็นเสมือนสมุดหน้าเหลือง (Yellow pages) สำหรับให้บุคลากรภาครัฐค้นหาแหล่งข้อมูลเพื่อใช้ประกอบการวิเคราะห์ หรือให้บริการได้อย่างสะดวก รวมไปถึงการออกแบบเครื่องมือต่าง ๆ ที่หน่วยงานภาครัฐต้องใช้ในการกำกับดูแลและให้บริการข้อมูลของหน่วยงานได้อย่างเป็นระบบ

๔. การพัฒนาระบบสารสนเทศเพื่อบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูลสำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และการให้บริการประชาชนแบบ One Stop Services ของหน่วยงานภาครัฐ โดยมีบริการพื้นฐาน เช่น การยืนยันตัวตน การจำกัดสิทธิในการเข้าถึงข้อมูล บริการส่งข้อมูลข้ามหน่วยงานผ่านระบบสารสนเทศ บันทึกธุรกรรม (Transaction) การเข้าถึงข้อมูลเพื่อเป็นหลักฐาน และการบริการข้อมูลประเภทอื่น

๕. การศึกษากระบวนการทางกฎหมายและกฎกระทรวงต่าง ๆ รวมทั้งศึกษาพระราชบัญญัติคุ้มครองส่วนบุคคล และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อออกแบบแนวทางปฏิบัติที่เหมาะสมเพื่อเอื้อให้เกิดประโยชน์ข้อมูลและการบูรณาการข้อมูลข้ามหน่วยงานได้อย่างเป็นรูปธรรม

๖. เป้าหมายระยะยาวของกรอบการวิเคราะห์ข้อมูลขนาดใหญ่ภาครัฐนี้คือ การที่กระทรวง รัฐวิสาหกิจ และส่วนราชการทุกแห่งมีศักยภาพในการจัดเก็บและประมวลผลข้อมูลได้อย่างเป็นระบบ รวมทั้งสามารถใช้ประโยชน์ข้อมูลขนาดใหญ่และเชื่อมโยง/แลกเปลี่ยนข้อมูลได้อย่างเป็นรูปธรรม เพื่อให้เกิดการให้บริการประชาชนที่มีประสิทธิภาพ พัฒนาศักยภาพการแข่งขันของอุตสาหกรรมโดยรวมและสร้างให้เกิดการบริหารราชการที่มีประสิทธิภาพ ต้นทุนลดลง และเพิ่มความโปร่งใสเป็นธรรม

๓.๒ สาระสำคัญของแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๒.๑ วัตถุประสงค์

๑) เพื่อกำหนดกรอบแนวนโยบายการจัดทำฐานข้อมูลด้านความมั่นคง

๒) เพื่อพัฒนาระบบข้อมูลในการติดตาม วิเคราะห์ ประเมินสถานการณ์ เพิ่มศักยภาพในการรับมือภัยคุกคาม ป้องกันแก้ไข ระงับ ยับยั้งปัญหาภัยคุกคามและภัยพิบัติ

๓) เพื่อเพิ่มประสิทธิภาพการแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานด้านความมั่นคงและหน่วยงานที่สนับสนุนภารกิจด้านความมั่นคงให้มีประสิทธิภาพ

๔) เพื่อบริหารจัดการข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอที่จะใช้ในการแก้ไขปัญหาความมั่นคงได้อย่างมีประสิทธิภาพ

๓.๒.๒ เป้าหมายและตัวชี้วัด

๑) เป้าหมาย

การมีระบบฐานข้อมูลและข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอสามารถสนับสนุนกลไกการตัดสินใจเพื่อแก้ไขปัญหาความมั่นคงในระดับชาติ

๒) ตัวชี้วัด

(๑) ระดับความสำเร็จการมีแผนฐานข้อมูลด้านความมั่นคง

(๒) ระดับความสำเร็จการพัฒนาระบบข้อมูลด้านความมั่นคงระหว่างหน่วยงาน

(๓) ระดับความสำเร็จการมีกลไกการแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานด้านความมั่นคง

(๔) ระดับความสำเร็จการบริหารจัดการข้อมูลด้านความมั่นคงเพื่อประกอบการเสนอแนะนโยบาย/แผนและแนวทางในการป้องกันและแก้ไขปัญหาความมั่นคง

๓.๒.๓ แนวทางการพัฒนา

๑) แนวทางการพัฒนาที่ ๑ นโยบายการบูรณาการฐานข้อมูลด้านความมั่นคง

(๑) ศึกษา ทบทวน ปรับปรุง นโยบาย แผน กฎ ระเบียบ ประกาศ คำสั่ง และแนวทางดำเนินงานของหน่วยงานที่เกี่ยวข้องกับฐานข้อมูลด้านความมั่นคง เพื่อเป็นกรอบนโยบายหรือแนวทางการจัดทำฐานข้อมูลด้านความมั่นคงมีความสอดคล้องกับยุทธศาสตร์ชาติ (พ.ศ. ๒๕๖๑ - ๒๕๘๐) และแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) รวมทั้งเกื้อหนุนการทำงานในเชิงบูรณาการฐานข้อมูลด้านความมั่นคง ตลอดจนมีกฎหมายที่คุ้มครองการปฏิบัติงานของเจ้าหน้าที่ โดยการประชุมหารือร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อวางแผนและจัดทำแผนรองรับให้มีความสอดคล้องกันทั้งในระดับนโยบายและระดับปฏิบัติ

(๒) เสริมสร้างและบูรณาการข้อมูลร่วมกันเพื่อสนับสนุนยุทธศาสตร์ชาติด้านความมั่นคง แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง การดำเนินนโยบายและแผนงานด้านความมั่นคง โดยประสาน

และบูรณาการการจัดทำร่วมกับกระทรวงมหาดไทย กระทรวงกลาโหม กระทรวงยุติธรรม กระทรวงการต่างประเทศ สำนักงานตำรวจแห่งชาติ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานที่เกี่ยวข้อง

(๓) สนับสนุนการมีฐานข้อมูลของหน่วยงานที่สอดคล้องกับสถานการณ์และสภาพปัญหาด้านความมั่นคง เพื่อนำข้อมูลมาใช้ในการบริหารจัดการเชิงป้องกันและแก้ไขปัญหาที่เกิดขึ้นตั้งแต่ก่อนเกิดเหตุ ขณะเกิดเหตุ และภายหลังเกิดเหตุ โดยกำหนดประเภทของข้อมูลที่จำเป็นต้องดำเนินการในจัดทำเป็นฐานข้อมูลด้านความมั่นคงในแต่ละห้วงเวลาที่ชัดเจน

(๔) กำหนดฐานข้อมูลด้านความมั่นคงในแต่ละประเภทและจัดการลำดับความเร่งด่วนในการจัดเก็บข้อมูล ทั้งนี้ ฐานข้อมูลที่จะดำเนินการต้องมีการจัดชั้นความลับอย่างเหมาะสมตามระเบียบและข้อกฎหมายที่เกี่ยวข้อง ตลอดจนเปิดโอกาสให้ผู้ที่ใช้ประโยชน์จากฐานข้อมูลทั้งในระดับนโยบายและระดับปฏิบัติสามารถนำไปใช้ได้อย่างมีประสิทธิภาพโดยความเห็นชอบจากคณะกรรมการที่จะจัดตั้งขึ้นต่อไป

๒) แนวทางการพัฒนาที่ ๒ การพัฒนาระบบฐานข้อมูลด้านความมั่นคง

(๑) พัฒนาระบบฐานข้อมูลด้านความมั่นคงทั้งในระดับนโยบายและระดับปฏิบัติที่เหมาะสมโดยให้ความสำคัญกับการจัดเก็บ รวบรวม วิเคราะห์ และนำข้อมูลมาใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

(๒) ส่งเสริมและสนับสนุนการจัดทำประเภทบัญชีข้อมูลด้านความมั่นคง (ไม่มีชั้นความลับและกำหนดชั้นความลับ) เพื่อประโยชน์ในการบริหารจัดการภัยคุกคามหรือปัญหาที่กระทบต่อความมั่นคงทุกรูปแบบ โดยวางแผนและทำการแลกเปลี่ยนข้อมูลกับหน่วยงานที่เกี่ยวข้อง เพื่อให้ข้อมูลมีความทันสมัยโดยใช้ประโยชน์จากช่องทางการติดต่อสื่อสารและการประสานงานที่รวดเร็วและมีประสิทธิภาพ

(๓) ส่งเสริม สนับสนุน พัฒนา เครื่องมือ อุปกรณ์ ระบบเทคโนโลยีที่ทันสมัยให้กับหน่วยงานที่มีหน้าที่ดำเนินการในกิจการงานความมั่นคง โดยจัดทำแผนความต้องการและแผนงบประมาณรองรับในกรอบยุทธศาสตร์การจัดสรรงบประมาณและแผนปฏิบัติราชการที่ชัดเจน

(๔) พัฒนาและวางแผนโครงสร้างอัตรากำลังและศักยภาพของบุคคลากรให้มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้าน ค่าตอบแทน แรงจูงใจ โดยวางแผนความต้องการกำลังคน การจัดสรรทุนการศึกษา อบรม และการพัฒนาประสิทธิภาพกำลังคนในสาขาที่เกี่ยวข้อง อาทิ ผู้บริหาร, Data Engineer, Data Scientist, Data Visualizer รวมทั้งให้มุ่งเน้นการพัฒนาการฝึกอบรมในลักษณะ Project Based Learning เพื่อให้สามารถปฏิบัติได้จริงมากกว่าเรียนรู้จากทฤษฎี

๓) แนวทางการพัฒนาที่ ๓ การดำเนินงานด้านเทคนิคเพื่อบูรณาการข้อมูลระหว่างหน่วยงาน

(๑) พัฒนาโครงสร้างพื้นฐานการจัดเก็บและประมวลผลหน่วยงานที่เกี่ยวข้องที่เหมาะสม มีประสิทธิผลในการใช้งานทั้งในมิติการรักษาความปลอดภัย การจัดหมวดหมู่ข้อมูล การแลกเปลี่ยนเชื่อมโยงข้อมูลอย่างเป็นระบบ

(๒) พัฒนาระบบสารสนเทศเพื่อบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูลสำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) และการให้บริการสาธารณะสำหรับข้อมูลทั่วไปแบบ One Stop Services ของหน่วยงานภาครัฐ โดยมีบริการพื้นฐาน เช่น การยืนยันตัวตน การจำกัดสิทธิในการเข้าถึง

ข้อมูล บริการส่งข้อมูลข้ามหน่วยงานผ่านระบบสารสนเทศ บันทึกธุรกรรม (Transaction) การเข้าถึงข้อมูลเพื่อเป็นหลักฐาน และการบริการข้อมูลประเภทอื่น เป็นต้น

(๓) พัฒนาระบบรายการข้อมูลภาครัฐ (Government Data Catalog) โดยรวบรวมรายละเอียดของข้อมูล (Metadata) สำคัญจากหน่วยงานภาครัฐทั้งหมดเพื่อจัดสร้างเป็นรายการ (Catalog) โดยแบ่งจัดทำเป็นระยะและพัฒนากลไกการสืบค้นในมิติต่าง ๆ และหน้าจอสืบค้นสำหรับบุคลากรภาครัฐ เพื่อให้ประกอบการวิเคราะห์รวมไปถึงการออกแบบเครื่องมือต่าง ๆ ที่หน่วยงานภาครัฐต้องใช้ในการกำกับดูแลบริหารข้อมูลของหน่วยงานได้อย่างเป็นระบบ

(๔) การจัดทำระบบวิเคราะห์และจัดทำรายงาน เพื่อให้สอดคล้องกับข้อเสนอ Platform ด้านความมั่นคงของกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

(๕) สนับสนุนการออกแบบตามกรอบแนวทางที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดขึ้น (สถาปัตยกรรมโครงสร้างพื้นฐานแบบแบ่งปันที่ผู้รับบริการมองเสมือนว่าเป็นโครงสร้างเดียวที่ใช้ร่วมกัน) ส่วนทางกายภาพโครงสร้างพื้นฐานเป็นแบบกระจายที่มีการเช่าใช้คลาวด์ผสมกับการสร้างดาต้าเซนเตอร์ หน่วยงานภาครัฐสามารถวางแผนการปรับโครงสร้างพื้นฐาน การประมวลผลที่เหมาะสมให้กับหน่วยงานได้ โดยทำการวิเคราะห์ช่องว่าง (Gap Analysis)

๔) แนวทางการพัฒนาที่ ๔ การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง

(๑) การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคงในระดับนโยบาย มอบให้ สภาความมั่นคงแห่งชาติ (โดย สำนักงานสภาความมั่นคงแห่งชาติ : สมช.) เป็นหน่วยรับผิดชอบ โดยให้แต่งตั้งคณะกรรมการบูรการฐานข้อมูลด้านความมั่นคง โดยมีรองนายกรัฐมนตรีที่นายกรัฐมนตรีมอบหมายเพื่อทำหน้าที่กำหนดนโยบายและแนวทางการบูรณาการฐานข้อมูลด้านความมั่นคงให้เป็นเอกภาพสำหรับการวิเคราะห์ คาดการณ์ วางแผนด้านความมั่นคงสนับสนุนการตัดสินใจของนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ ในการบริหารราชการแผ่นดินตลอดจนกำกับ ติดตามการดำเนินงานเรื่องดังกล่าว

(๒) การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในระดับอำนวยการและประสานการปฏิบัติ มอบให้ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) เป็นหน่วยงานกลางรับผิดชอบทำหน้าที่เป็น**ศูนย์กลางข้อมูลด้านความมั่นคง (Data Center)** โดยประสานและบูรณาการข้อมูลตลอดจนทำการเชื่อมโยงแลกเปลี่ยนข้อมูลกับศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) หรือศูนย์ต่าง ๆ และหน่วยงานที่เกี่ยวข้องเพื่อนำข้อมูลเสนอสภาความมั่นคงแห่งชาติ โดยให้หน่วยงานที่เกี่ยวข้องกับแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคงให้การสนับสนุนและนำเข้าข้อมูลแก่กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร อาทิ กระทรวงมหาดไทย กระทรวงกลาโหม กระทรวงยุติธรรม กระทรวงการต่างประเทศ สำนักงานตำรวจแห่งชาติ เพื่อให้มีข้อมูลที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอที่จะใช้ในการป้องกันและแก้ไขปัญหาความมั่นคงได้อย่างมีประสิทธิภาพ

(๓) กระทรวง/กรม ที่เกี่ยวข้องในระดับปฏิบัติสนับสนุนข้อมูลและแลกเปลี่ยนเชื่อมโยงให้กับศูนย์กลางข้อมูลด้านความมั่นคง สำหรับกระทรวง/กรม ที่เกี่ยวข้องกับข้อมูลสถานการณ์ทางทะเล (นอกเหนือจาก ๖ หน่วยงาน ได้แก่ กองทัพเรือ กองบังคับการตำรวจน้ำ กรมประมง กรมเจ้าท่า กรมศุลกากร และ

กรมทรัพยากรทางทะเลและชายฝั่ง) สนับสนุนข้อมูลให้ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) เพื่อประมวลผลก่อนส่งให้ศูนย์กลางข้อมูลด้านความมั่นคง (Big Data) ใช้ประโยชน์ต่อไป

(๔) การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในการรักษาความมั่นคงภายในประเทศ มอบให้ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) เป็นหน่วยงานรับผิดชอบดำเนินการโดยประสานกับกองอำนวยการรักษาความมั่นคงภายในภาค (กอ.รมน.ภาค) และกองอำนวยการรักษาความมั่นคงภายในจังหวัด (กอ.รมน.จังหวัด)

(๕) การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในการรักษาความมั่นคงทางทะเล มอบให้ ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) เป็นหน่วยงานรับผิดชอบดำเนินการร่วมกับหน่วยงานภายในศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล และหน่วยงานที่เกี่ยวข้องโดยประสานกับศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเลภาค (ศรชล.ภาค) และศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเลจังหวัด (ศรชล.จังหวัด) ทั้งนี้ ให้ประสานกับกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรในฐานะหน่วยงานกลางบูรณาการข้อมูลด้านความมั่นคง

(๖) การจัดทำข้อมูลเพื่อการระดมสรรพกำลัง การกำลังสำรอง และการสัสดี มอบให้กระทรวงกลาโหม เป็นหน่วยงานหลักบูรณาการข้อมูลภายในกระทรวงกลาโหมและหน่วยงานที่เกี่ยวข้อง เพื่อสนับสนุนภารกิจการป้องกันประเทศ

(๗) การส่งเสริมความร่วมมือ/ความตกลงเพื่อให้มีการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงานสามารถจัดทำเป็นบันทึกความเข้าใจว่าด้วยการเชื่อมโยงฐานข้อมูล (Memorandum of Understanding : MOU) อาทิ กระทรวงมหาดไทย กระทรวงกลาโหม กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) สำนักงานสภาความมั่นคงแห่งชาติ สำนักงานตำรวจแห่งชาติ และหน่วยงานที่เกี่ยวข้อง

(๘) การติดตามและประเมินผล มอบให้สำนักงานสภาความมั่นคงแห่งชาติร่วมกับกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร และศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) รับผิดชอบดำเนินการ

๓.๒.๔ ปัจจัยแห่งความสำเร็จ

๑) นโยบายการบูรณาการข้อมูลด้านความมั่นคงต้องมีความต่อเนื่อง โดยรัฐบาลให้การสนับสนุนแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง รวมทั้งให้การสนับสนุนทรัพยากรเพื่อขับเคลื่อนงานอย่างเป็นรูปธรรม

๒) หน่วยงานที่เกี่ยวข้องทุกหน่วยงานให้ความร่วมมือในการเชื่อมต่อและแบ่งปันข้อมูลภายใน Platform ด้านความมั่นคง รวมทั้งปรับปรุงระบบข้อมูลให้มีความทันสมัยสามารถนำมาใช้งาน เพื่อแลกเปลี่ยนข้อมูลระหว่างหน่วยงานได้อย่างทันท่วงทีเมื่อเกิดสถานการณ์

๓) การพัฒนาศักยภาพบุคลากร (Peopleware) ด้านเทคโนโลยีสารสนเทศของทุกหน่วยงานที่เกี่ยวข้องให้มีความเชี่ยวชาญสอดคล้องตามภารกิจที่ดำเนินการอย่างต่อเนื่อง และมีจำนวนเพียงพอต่อการปฏิบัติงาน

๓.๓ โครงการสำคัญ (สาระสำคัญ/หน่วยดำเนินการ/กรอบเวลาดำเนินการ)

๓.๓.๑ โครงการบูรณาการข้อมูลด้านการเตรียมพร้อมแห่งชาติ

๑) **สาระสำคัญ** การจัดทำระบบฐานข้อมูลสารสนเทศเพื่อสนับสนุนการพัฒนาศักยภาพระบบการเตรียมพร้อมแห่งชาติ โดยให้ความสำคัญกับการแลกเปลี่ยนข้อมูลด้านความมั่นคงระหว่างหน่วยงานที่มีภารกิจเกี่ยวข้องกับการเตรียมความพร้อมของชาติ เพื่อให้เกิดระบบการเตรียมพร้อมที่มีศักยภาพสามารถจัดการกับภาวะไม่ปกติและจัดการความเสี่ยงได้อย่างบูรณาการ นอกจากนี้ ยังให้ความสำคัญกับการเพิ่มประสิทธิภาพของระบบฐานข้อมูล และการพัฒนาบุคลากรภาครัฐเพื่อสนับสนุนการวิเคราะห์ข้อมูลของระบบดังกล่าว

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กระทรวงกลาโหม กระทรวงมหาดไทย (กรมป้องกันและบรรเทาสาธารณภัย) กระทรวงการต่างประเทศ กระทรวงสาธารณสุข กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงแรงงาน กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานอื่น ๆ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) โครงการพัฒนาระบบสารสนเทศเพื่อการระดมสรรพกำลัง (กรมการสรรพกำลังกลาโหม)

(๒) โครงการพัฒนาระบบสารสนเทศเพื่อการกำลังสำรองและการสัสดี (กรมการสรรพกำลังกลาโหม)

(๓) ระบบบริหารจัดการข้อมูลในภาวะวิกฤติ (Crisis Information Management System) (กรมป้องกันและบรรเทาสาธารณภัย)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๒ โครงการบูรณาการข้อมูลด้านการบริหารจัดการชายแดน

๑) **สาระสำคัญ** การจัดทำระบบฐานข้อมูลสารสนเทศที่สนับสนุนการบริหารจัดการชายแดนด้านความมั่นคง โดยให้ความสำคัญกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลความมั่นคงระหว่างหน่วยงานที่มีภารกิจบริหารจัดการชายแดน เพื่อบูรณาการการป้องกันและแก้ไขปัญหาที่เกิดขึ้นบริเวณชายแดนร่วมกันในทุกระดับทั้งในภาวะสถานการณ์ปกติและสถานการณ์วิกฤติ รวมทั้งทำให้พื้นที่ชายแดนมีความมั่นคงปลอดภัยสามารถรองรับปัญหาความมั่นคงในรูปแบบต่าง ๆ นอกจากนี้ ยังให้ความสำคัญกับการเพิ่มประสิทธิภาพของระบบฐานข้อมูลและการพัฒนาบุคลากรภาครัฐเพื่อสนับสนุนการวิเคราะห์ข้อมูลของระบบดังกล่าว

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กระทรวงกลาโหม (กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงการคลัง (กรมศุลกากร) กระทรวงคมนาคม กระทรวงมหาดไทย (กรมการปกครองและกรมป้องกันและบรรเทาสาธารณภัย) กระทรวงแรงงาน กระทรวงการต่างประเทศ (กรมการกงสุล) สำนักงานตำรวจแห่งชาติ (สำนักงานตรวจคนเข้าเมือง) และสำนักงานสภาความมั่นคงแห่งชาติ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) ระบบการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (LINKAGE CENTER) (กรมการปกครอง)

(๒) ระบบการเชื่อมโยงข้อมูลทะเบียนประวัติราษฎร (IKNO) (กรมการปกครอง)

(๓) ฐานข้อมูลการตรวจลงตรา (กรมการกงสุล)

(๔) ฐานข้อมูลหนังสือเดินทาง (กรมการกงสุล)

(๕) ฐานข้อมูลสินค้าเข้า - ออก และฐานข้อมูลของต้องห้าม - ของต้องจำกัด (กรมศุลกากร)

(๖) ฐานข้อมูลทะเบียนรถ (กระทรวงคมนาคม)

(๗) สถิติการค้าชายแดน (มูลค่าการค้าชายแดน ประเภทสินค้าที่มีการส่งออก - นำเข้าสูงสุด) (กรมศุลกากร)

(๘) ข้อมูลแรงงานต่างด้าวสัญชาติเมียนมา ลาว และกัมพูชา (กระทรวงแรงงาน)

(๙) ข้อมูลการเดินทาง (สำนักงานตรวจคนเข้าเมือง)

(๑๐) ข้อมูลการขออยู่ต่อ (สำนักงานตรวจคนเข้าเมือง)

(๑๑) ข้อมูลบุคคลต้องห้าม (สำนักงานตรวจคนเข้าเมือง)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๓ โครงการบูรณาการข้อมูลด้านการรักษาผลประโยชน์ของชาติทางทะเล

๑) **สาระสำคัญ** การจัดทำระบบฐานข้อมูลสารสนเทศที่สนับสนุนการป้องกันและแก้ไขปัญหาด้านการรักษาผลประโยชน์ของชาติทางทะเลตามภารกิจของหน่วยงานให้เป็นระบบที่ตอบสนองต่อการใช้งานทั้งภายในพื้นที่ทะเลอาณาเขตและเขตเศรษฐกิจจำเพาะ สำหรับการแลกเปลี่ยนและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานที่ปฏิบัติงานกับหน่วยงานระดับนโยบายส่วนกลางได้อย่างรวดเร็ว นอกจากนี้ มีการเชื่อมโยงฐานข้อมูลสำคัญระหว่างหน่วยงานในพื้นที่และหน่วยงานส่วนกลางในด้านข้อมูลด้านแหล่งทรัพยากรทางทะเล การผ่านน่านน้ำไทยของเรือธงประเทศไทยและธงต่างประเทศ การเคลื่อนย้ายถิ่นฐานแบบไม่ปกติและการกระทำที่จะเป็นอาชญากรรมทางทะเลที่ส่งผลต่อการสนับสนุนการตกลงใจในระดับนโยบายและมีการเพิ่มขีดความสามารถของระบบเทคโนโลยีสารสนเทศ ทรัพยากรบุคคล และการบริหารจัดการให้สามารถรองรับภารกิจงานบูรณาการฐานข้อมูลด้านความมั่นคงดังกล่าว

๒) **หน่วยงานหลักที่เกี่ยวข้อง** ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล กระทรวงกลาโหม (กองทัพเรือ) กระทรวงเกษตรและสหกรณ์ กระทรวงคมนาคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงแรงงาน กระทรวงการต่างประเทศ (กรมการกงสุล) สำนักงานตำรวจแห่งชาติ (สำนักงานตรวจคนเข้าเมือง) และสำนักงานสภาความมั่นคงแห่งชาติ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) โครงการพัฒนาระบบวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เพื่อการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.)

(๒) ระบบแก้ปัญหาการประมงผิดกฎหมาย ขาดการรายงาน และไร้การควบคุม (IUU) (กรมประมง)

(๓) การจัดทำข้อมูลและฐานข้อมูลเรือ (ศรชล./กรมเจ้าท่า/กรมประมง)

(๔) การจัดระเบียบการเข้า - ออกทางทะเล (ศรชล./กรมเจ้าท่า/กรมประมง)

(๕) ข้อมูลทะเบียนเรือไทย (กระทรวงคมนาคม)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๔ **โครงการบูรณาการข้อมูลด้านปัญหาอาชญากรรมข้ามชาติและการก่อการร้าย**

๑) **สาระสำคัญ** การจัดทำระบบฐานข้อมูลสารสนเทศที่สนับสนุนการป้องกันและแก้ไขปัญหาอาชญากรรมข้ามชาติตามภารกิจของหน่วยงานให้เป็นระบบที่ตอบสนองต่อการใช้งานทั้งภายในและภายนอกประเทศ พร้อมทั้งเชื่อมโยงและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานทั้งในระดับนโยบายและระดับปฏิบัติตามความเหมาะสม เพื่อให้เกิดประสิทธิภาพในการรวบรวม วิเคราะห์ และนำข้อมูลมาใช้ในการป้องกันและแก้ไขปัญหาอาชญากรรมข้ามชาติ

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กระทรวงยุติธรรม กระทรวงมหาดไทย (กรมการปกครอง) กระทรวงแรงงาน กระทรวงการต่างประเทศ (กรมการกงสุล) สำนักงานตำรวจแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด และหน่วยงานอื่น ๆ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) ระบบฐานข้อมูลอาชญากรรมและอาชญากรรมข้ามชาติขององค์การตำรวจสากล “I-24/7” (สำนักงานตำรวจแห่งชาติ)

(๒) ฐานข้อมูลรายการประวัติหนังสือเดินทางและฐานข้อมูลการตรวจลงตรา (กรมการกงสุล)

(๓) ฐานข้อมูลผู้ต้องขัง (กระทรวงยุติธรรม)

(๔) ฐานข้อมูลกลุ่มต่อต้านประเทศเพื่อนบ้าน (สำนักงานตำรวจแห่งชาติ)

(๕) ฐานข้อมูลกลุ่มองค์การพัฒนาเอกชนต่างประเทศที่ได้รับอนุญาตให้ตั้งสำนักงานในประเทศหรือดำเนินงานในประเทศไทย (สำนักงานตำรวจแห่งชาติ)

(๖) ฐานข้อมูลการตรวจสอบพฤติการณ์บุคคล (สำนักงานตำรวจแห่งชาติ)

(๗) ฐานข้อมูลตรวจสอบประวัติบุคคลต่างด้าวที่เกี่ยวข้องกับการก่อการร้ายสากล (สำนักงานตำรวจแห่งชาติ)

(๘) ฐานข้อมูลนักรบต่างชาติ (สำนักงานตำรวจแห่งชาติ)

(๙) ฐานข้อมูลบุคคลกลุ่มบุคคลสนับสนุนทางการเงินให้กับองค์ก่อการร้ายสากล (สำนักงานตำรวจแห่งชาติ)

(๑๐) ฐานข้อมูลการเดินทางเข้าออกประเทศไทย (สำนักงานตำรวจแห่งชาติ)

(๑๑) ฐานข้อมูลการขอสัญชาติไทยของชาวต่างชาติ (สำนักงานตำรวจแห่งชาติ)

(๑๒) ฐานข้อมูลการขอวีซ่าเข้าประเทศไทย (กรมการกงสุล/สำนักงานตรวจคนเข้าเมือง)

(๑๓) ระบบการสืบค้นข้อมูลหมายจับในรูปแบบเว็บเซอร์วิส (Web Service) (สำนักงานตำรวจแห่งชาติ)

(๑๔) ระบบการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (LINKAGE CENTER) (กรมการปกครอง)

(๑๕) ระบบการเชื่อมโยงข้อมูลทะเบียนประวัติราษฎร (IKNO) (กรมการปกครอง)

(๑๖) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือ (AFIS) (กรมการปกครอง)

(๑๗) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยภาพ (Face Recognition) (กรมการปกครอง)

(๑๘) ข้อมูลรายชื่อบุคคลที่ถูกกำหนดตามมติหรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติ (UN list) และข้อมูลรายชื่อที่ถูกกำหนดที่ศาลแพ่งมีคำสั่ง (Thai List) (สำนักงาน ปปง.)

(๑๙) ข้อมูลหมายจับตำรวจสากล (สำนักงานตำรวจแห่งชาติ)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๕ **โครงการบูรณาการข้อมูลด้านปัญหาผู้หลบหนีเข้าเมือง**

๑) **สาระสำคัญ** มุ่งเน้นการจัดทำระบบฐานข้อมูลสารสนเทศที่สนับสนุนการแก้ไขปัญหาด้านการหลบหนีเข้าเมืองหรือการเข้าเมืองแบบผิดกฎหมายตามภารกิจของหน่วยงานให้เป็นระบบที่ตอบสนองต่อการใช้งานทั้งภายในและภายนอกประเทศ สำหรับการแลกเปลี่ยนและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานที่ปฏิบัติงานกับหน่วยงานระดับนโยบายส่วนกลางได้อย่างรวดเร็ว นอกจากนี้ ยังมีการเชื่อมโยงฐานข้อมูลสำคัญระหว่างหน่วยงานในพื้นที่และหน่วยงานส่วนกลางในด้านการหลบหนีเข้าเมือง การเข้าเมืองแบบผิดกฎหมายที่สามารถสนับสนุนการตกลงใจในระดับนโยบายและมีการเพิ่มขีดความสามารถของระบบเทคโนโลยีสารสนเทศ ทรัพยากรบุคคล และการบริหารจัดการให้สามารถรองรับภารกิจงานบูรณาการฐานข้อมูลด้านความมั่นคงดังกล่าว

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) สำนักงานตำรวจแห่งชาติ (สำนักงานตรวจคนเข้าเมือง) กระทรวงมหาดไทย (กรมการปกครอง) กระทรวงกลาโหม (กองทัพบก) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงแรงงาน กระทรวงการต่างประเทศ (กรมการกงสุล) และสำนักงานสภาความมั่นคงแห่งชาติ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) ระบบแจ้งเตือนและระบบเฝ้าตรวจทั้งทางบกและทางทะเลในลักษณะเครือข่าย (Network) (กอ.รมน.)

(๒) การจัดทำระบบฐานข้อมูลผู้หลบหนีเข้าเมือง คนต่างด้าว ระหว่างส่วนราชการ โดยจำแนกกลุ่มเป้าหมาย ๔ กลุ่ม ได้แก่ (๑) กลุ่มที่มีปัญหาสถานะทางทะเบียน (๒) กลุ่มแรงงานต่างด้าวผิดกฎหมาย (๓) กลุ่มผู้หลบหนีเข้าเมืองกลุ่มเฉพาะ อาทิ โรฮีนยา เกาหลีเหนือ และ (๔) กลุ่มผู้หลบหนีเข้าเมืองกลุ่มอื่น ๆ (กอ.รมน.)

(๓) ข้อมูลที่พักแรมและคนเข้าเมือง (กอ.รมน.)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๖ **โครงการบูรณาการข้อมูลด้านอัตลักษณ์**

๑) **สาระสำคัญ** การจัดทำระบบฐานข้อมูลสารสนเทศที่สนับสนุนการบูรณาการข้อมูลอัตลักษณ์บุคคลของประเทศให้เป็นมาตรฐานเดียวกัน มีความถูกต้องแม่นยำ และสามารถแลกเปลี่ยนข้อมูลร่วมกันภายใต้ระบบความปลอดภัยข้อมูลอัตลักษณ์บุคคลที่มีประสิทธิภาพ รวมทั้งสามารถสนับสนุนกระบวนการยุติธรรมได้อย่างเป็นธรรมและรวดเร็ว

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กระทรวงยุติธรรม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงมหาดไทย สำนักงานสภาความมั่นคงแห่งชาติ สำนักข่าวกรองแห่งชาติ สำนักงานตำรวจแห่งชาติ กรมการกงสุล กรมการปกครอง และหน่วยงานอื่นๆ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) ระบบฐานข้อมูลดีเอ็นเอ (กระทรวงยุติธรรม)

(๒) ระบบฐานข้อมูลลายพิมพ์นิ้วมือ (กระทรวงยุติธรรม)

(๓) ระบบฐานข้อมูลคนหายและศพนิรนาม (กระทรวงยุติธรรม)

(๔) ระบบฐานข้อมูลการตรวจพิสูจน์ทางนิติวิทยาศาสตร์ (กระทรวงยุติธรรม)

(๕) ระบบศูนย์กลางการแลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center) (กระทรวงยุติธรรม)

(๖) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือ (Automated fingerprint identification systems : AFIS) (กรมการปกครอง)

(๗) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยภาพใบหน้า (Face Recognition) (กรมการปกครอง)

(๘) ฐานข้อมูลด้านนิติวิทยาศาสตร์ (สำนักงานตำรวจแห่งชาติ)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๗ **โครงการบูรณาการฐานข้อมูลด้านการแก้ไขปัญหาพื้นที่ ๓ จังหวัดชายแดนภาคใต้**

๑) **สาระสำคัญ** การจัดระบบฐานข้อมูลสารสนเทศที่สนับสนุนการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ ตามภารกิจของหน่วยงานให้เป็นระบบที่ทันสมัยพร้อมใช้งานได้ทุกสถานการณ์ พร้อมทั้งสนับสนุนการพัฒนาฐานข้อมูลด้านความมั่นคงจังหวัดชายแดนภาคใต้สำหรับการแลกเปลี่ยนและใช้ประโยชน์ข้อมูลร่วมกันระหว่างหน่วยงานในระดับพื้นที่กับหน่วยงานระดับนโยบายในส่วนกลางได้อย่างรวดเร็ว และปลอดภัย นอกจากนี้ ยังเชื่อมโยงฐานข้อมูลสำคัญระหว่างหน่วยงานในพื้นที่และหน่วยงานส่วนกลางให้สามารถสนับสนุนการตกลงใจในระดับนโยบาย และมีความพร้อมสำหรับการบัญชาการเหตุการณ์ทั้งในสถานการณ์ปกติและสถานการณ์ฉุกเฉิน

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กระทรวงยุติธรรม กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ กรมการปกครอง กองทัพอากาศ สำนักงานตำรวจแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ และหน่วยงานอื่น ๆ

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

(๑) โครงการบูรณาการจัดทำข้อมูลกลางความมั่นคงจังหวัดชายแดนภาคใต้ (กอ.รมน.)

(๒) โครงการถ่ายภาพถ่ายทางอากาศสนับสนุนการบูรณาการฐานข้อมูลด้านความมั่นคงจังหวัดชายแดนภาคใต้ (กองทัพอากาศ)

(๓) ระบบฐานข้อมูล Crimes (สำนักงานตำรวจแห่งชาติ)

(๔) ข้อมูลพิมพ์ลายนิ้วมือ ฝ่ามือ สันมือ ของบุคคลพ้นโทษจังหวัดชายแดนภาคใต้ (สำนักงานตำรวจแห่งชาติ)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๘ **โครงการบูรณาการข้อมูลด้านการข่าว**

๑) **สาระสำคัญ** การพัฒนาระบบฐานข้อมูลด้านการข่าว เพื่อพัฒนาระบบสารสนเทศมาสนับสนุนการดำเนินการงานภายในของศูนย์ประสานข่าวกรองแห่งชาติทั้งในระดับบริหารและระดับปฏิบัติการ เพิ่มศักยภาพการทำงาน ลดขั้นตอนและระยะเวลาการดำเนินงาน เป็นศูนย์กลางข้อมูลและการเชื่อมโยงข้อมูลข่าวสาร การติดต่อสื่อสารข้อมูลต่าง ๆ

๒) **หน่วยงานหลักที่เกี่ยวข้อง** หน่วยงานในประชาคมข่าวกรอง

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

- โครงการพัฒนาระบบฐานข้อมูลด้านการข่าว (สขช.)

๔) **กรอบระยะเวลาดำเนินการ** ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๓.๓.๙ **โครงการบูรณาการข้อมูลด้านการป้องกันและปราบปรามการค้ามนุษย์**

๑) **สาระสำคัญ** พัฒนาระบบฐานข้อมูลของประเทศไทยด้านการดำเนินคดี และการช่วยเหลือผู้เสียหายจากการค้ามนุษย์ สนับสนุนการป้องกันและแก้ไขปัญหาการค้ามนุษย์ตามภารกิจของหน่วยงานที่เกี่ยวข้อง โดยให้การจัดเก็บและการใช้ข้อมูลเป็นไปในทิศทางเดียวกัน ทั้งในระดับหน่วยงานและภาพรวมของประเทศ และเพื่อให้เกิดการบูรณาการข้อมูลสารสนเทศระหว่างหน่วยงานที่เกี่ยวข้องอย่างยั่งยืน รวมทั้งเพื่อประโยชน์ในการกำหนดนโยบายของประเทศไทย ด้านการดำเนินคดีและบังคับใช้กฎหมาย และการคุ้มครองช่วยเหลือผู้เสียหาย

๒) **หน่วยงานหลักที่เกี่ยวข้อง** กระทรวงยุติธรรม สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ กรมการปกครอง และสำนักงานปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

- ระบบฐานข้อมูลของประเทศไทยด้านการดำเนินคดี และการช่วยเหลือผู้เสียหายจากการค้ามนุษย์

๔) **กรอบระยะเวลาดำเนินการ** 5 ปี (พ.ศ. 2563 - 2567)

๓.๓.๑๐ **โครงการบูรณาการข้อมูลด้านอื่น ๆ**

๑) **สาระสำคัญ**

๒) **หน่วยงานหลักที่เกี่ยวข้อง**

๓) **โครงการ/ระบบ/ข้อมูลของหน่วยงานที่เกี่ยวข้องที่ร่วมบูรณาการ**

๔) **กรอบระยะเวลาดำเนินการ**

บัญชีข้อมูลด้านความมั่นคงของหน่วยงาน

โครงสร้างบัญชีข้อมูลด้านความมั่นคงของหน่วยงาน แบ่งเป็นกลุ่มหรือประเภทตามหน่วยงานต่าง ๆ

ประเภทข้อมูล/หน่วยงาน	คำอธิบายข้อมูล
๑. ข้อมูลด้านการเตรียมพร้อมแห่งชาติ	
๑.๑ กระทรวงกลาโหม ๑) โครงการพัฒนาระบบสารสนเทศเพื่อการระดมสรรพกำลัง ๒) โครงการพัฒนาระบบสารสนเทศเพื่อการกำลังสำรองและการสัสดี	
๑.๒ กรมป้องกันและบรรเทาสาธารณภัย • ระบบบริหารจัดการข้อมูลในภาวะวิกฤติ (Crisis Information Management System)	
๒. ข้อมูลด้านการบริหารจัดการชายแดน	
๒.๑ กระทรวงมหาดไทย (กรมการปกครอง) ๑) ระบบการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (LINKAGE CENTER) ๒) ระบบการเชื่อมโยงข้อมูลทะเบียนประวัติราษฎร (IKNO)	
๒.๒ กระทรวงการต่างประเทศ (กรมการกงสุล) ๑) ฐานข้อมูลการตรวจลงตรา ๒) ฐานข้อมูลหนังสือเดินทาง	
๒.๓ กระทรวงการคลัง (กรมศุลกากร) ๑) ฐานข้อมูลสินค้าเข้า - ออก และฐานข้อมูลของต้องห้าม - ของต้องจำกัด ๒) สถิติการค้าชายแดน (มูลค่าการค้าชายแดน ประเภทสินค้าที่มีการส่งออก - นำเข้าสูงสุด)	
๒.๔ กระทรวงแรงงาน (กรมการจัดหางาน) • ข้อมูลแรงงานต่างด้าวสัญชาติเมียนมา ลาว และกัมพูชา	

ประเภทข้อมูล/หน่วยงาน	คำอธิบายข้อมูล
๒.๕ กระทรวงคมนาคม (กรมการขนส่งทางบก) • ฐานข้อมูลทะเบียนรถ	
๒.๖ สำนักงานตรวจคนเข้าเมือง ๑) ข้อมูลการเดินทาง ๒) ข้อมูลการขออยู่ต่อ ๓) ข้อมูลบุคคลต้องห้าม	
๓. ข้อมูลด้านการรักษาผลประโยชน์ของชาติทางทะเล	
๓.๑ ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล ๑) โครงการพัฒนาระบบวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) เพื่อการรักษาผลประโยชน์ของชาติทางทะเล ๒) การจัดทำข้อมูลและฐานข้อมูลเรือ ๓) การจัดระเบียบการเข้า - ออกทางทะเล	
๓.๒ กระทรวงเกษตรและสหกรณ์ (กรมประมง) ๑) ระบบแก้ปัญหาการประมงผิดกฎหมาย ขาดการรายงาน และไร้การควบคุม (IUU) ๒) การจัดทำข้อมูลและฐานข้อมูลเรือ ๓) การจัดระเบียบการเข้า - ออกทางทะเล	
๓.๓ กระทรวงคมนาคม (กรมเจ้าท่า) ๑) ข้อมูลทะเบียนเรือไทย ๒) การจัดทำข้อมูลและฐานข้อมูลเรือ ๓) การจัดระเบียบการเข้า - ออกทางทะเล	
๔. ข้อมูลด้านปัญหาอาชญากรรมข้ามชาติและการก่อการร้าย	
๔.๑ สำนักงานตำรวจแห่งชาติ ๑) ระบบฐานข้อมูลอาชญากรรมและอาชญากรรมข้ามชาติขององค์การตำรวจสากล “I-24/7”	

ประเภทข้อมูล/หน่วยงาน	คำอธิบายข้อมูล
๒) ระบบการสืบค้นข้อมูลหมายจับในรูปแบบเว็บเซอร์วิส (Web Service) ๓) ฐานข้อมูลกลุ่มต่อต้านประเทศเพื่อนบ้าน ๔) ฐานข้อมูลกลุ่มองค์การพัฒนาเอกชนต่างประเทศที่ได้รับอนุญาตให้ตั้งสำนักงานในประเทศหรือดำเนินงานในประเทศไทย ๕) ฐานข้อมูลการตรวจสอบพฤติการณ์บุคคล ๖) ฐานข้อมูลตรวจสอบประวัติบุคคลต่างด้าวที่เกี่ยวข้องกับการก่อการร้ายสากล ๗) ฐานข้อมูลนักรบต่างชาติ ๘) ฐานข้อมูลบุคคลกลุ่มบุคคลสนับสนุนทางการเงินให้กับองค์ก่อการร้ายสากล ๙) ฐานข้อมูลการเดินทางเข้าออกประเทศไทย ๑๐) ฐานข้อมูลการขอสัญชาติไทยของชาวต่างชาติ ๑๑) ข้อมูลหมายจับตำรวจสากล	
๔.๒ สำนักงานตรวจคนเข้าเมือง • ฐานข้อมูลการขอวีซ่าเข้าประเทศไทย	
๔.๓ กระทรวงการต่างประเทศ (กรมการกงสุล) ๑) ฐานข้อมูลรายการประวัติหนังสือเดินทางและฐานข้อมูลการตรวจลงตรา ๒) ฐานข้อมูลการขอวีซ่าเข้าประเทศไทย	
๔.๔ กระทรวงยุติธรรม • ฐานข้อมูลผู้ต้องขัง	
๔.๕ กระทรวงมหาดไทย (กรมการปกครอง) ๑) ระบบการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (LINKAGE CENTER) ๒) ระบบการเชื่อมโยงข้อมูลทะเบียนประวัติราษฎร (IKNO) ๓) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือ (AFIS) ๔) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยภาพ (Face Recognition)	
๔.๖ สำนักงานป้องกันและปราบปรามการฟอกเงิน • ข้อมูลรายชื่อบุคคลที่ถูกกำหนดตามมติหรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติ (UN list) และข้อมูลรายชื่อที่ถูกกำหนดที่ศาลแพ่งมีคำสั่ง (Thai List)	

ประเภทข้อมูล/หน่วยงาน	คำอธิบายข้อมูล
๕. ข้อมูลด้านปัญหาผู้หลบหนีเข้าเมือง	
● สำนักงานตรวจคนเข้าเมือง ๑) ระบบแจ้งเตือน และระบบเฝ้าตรวจทั้งทางบกและทางทะเลในลักษณะเครือข่าย (Network) ๒) การจัดทำระบบฐานข้อมูลผู้หลบหนีเข้าเมือง คนต่างด้าวระหว่างส่วนราชการ โดยจำแนกกลุ่มเป้าหมาย ๔ กลุ่ม ได้แก่ (๑) กลุ่มที่มีปัญหาสถานะทางทะเบียน (๒) กลุ่มแรงงานต่างด้าวผิดกฎหมาย (๓) กลุ่มผู้หลบหนีเข้าเมืองกลุ่มเฉพาะ อาทิ โรฮีนจา เกาหลีเหนือ และ (๔) กลุ่มผู้หลบหนีเข้าเมืองกลุ่มอื่น ๆ ๓) ข้อมูลที่พักแรมและคนเข้าเมือง	
๖. ข้อมูลด้านอัตลักษณ์	
๖.๑ กระทรวงยุติธรรม ๑) ระบบฐานข้อมูลดีเอ็นเอ ๒) ระบบฐานข้อมูลลายพิมพ์นิ้วมือ ๓) ระบบฐานข้อมูลคนหายและศพนิรนาม ๔) ระบบฐานข้อมูลการตรวจพิสูจน์ทางนิติวิทยาศาสตร์	
๖.๒ กระทรวงมหาดไทย (กรมการปกครอง) ๑) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือ (Automated fingerprint identification systems : AFIS) ๒) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยภาพใบหน้า (Face Recognition)	
๖.๓ สำนักงานตำรวจแห่งชาติ ● ฐานข้อมูลด้านนิติวิทยาศาสตร์	
๗. ข้อมูลด้านการแก้ไขปัญหาพื้นที่ ๓ จังหวัดชายแดนภาคใต้	
๗.๑ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร ● โครงการบูรณาการจัดทำข้อมูลกลางความมั่นคง จชต.	

ประเภทข้อมูล/หน่วยงาน	คำอธิบายข้อมูล
๗.๒ กระทรวงกลาโหม (กองทัพอากาศ) ● โครงการถ่ายภาพถ่ายทางอากาศสนับสนุนการบูรณาการฐานข้อมูลด้านความมั่นคง จชต.	
๗.๓ สำนักงานตำรวจแห่งชาติ ๑) ระบบฐานข้อมูล Crimes ๒) ข้อมูลพิมพ์ลายนิ้วมือ ฝ่ามือ สันมือ ของบุคคลพ้นโทษ จชต.	
๗.๔ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ๑) โครงการแผ่นดินเดียวกัน (การแลกเปลี่ยนวัฒนธรรมของเด็กในพื้นที่สามจังหวัดชายแดนภาคใต้) ๒) โครงการส่งเสริมการดำเนินงานตามอนุสัญญาว่าด้วยสิทธิเด็ก (เด็กในบริบทโยกย้ายถิ่นฐาน)	
๘. โครงการบูรณาการข้อมูลด้านการข่าว สำนักข่าวกรองแห่งชาติ ● โครงการพัฒนาระบบฐานข้อมูลด้านการข่าว	
๙. โครงการบูรณาการข้อมูลด้านการป้องกันและปราบปรามการค้ามนุษย์ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ● ระบบฐานข้อมูลของประเทศไทยด้านการดำเนินคดี และการช่วยเหลือผู้เสียหายจากการค้ามนุษย์	
๑๐. โครงการบูรณาการข้อมูลด้านอื่น ๆ	

ข้อเสนอ Platform ด้านความมั่นคง

โดย

คณะทำงานด้านเทคนิคจัดทำ Platform ด้านความมั่นคง

สารบัญ

ภาคผนวก

บทสรุปผู้บริหาร

สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ.๒๕๖๓ - ๒๕๖๕) สำหรับใช้เป็นกรอบแนวทางในการบูรณาการข้อมูลด้านความมั่นคง ให้มีประสิทธิภาพ เพื่อสนับสนุนการแก้ไขปัญหาความมั่นคงได้ทุกมิติและทุกรูปแบบ ตามที่ยุทธศาสตร์ชาติด้านความมั่นคง และแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ให้ความสำคัญ โดยกำหนดกรอบแนวทางการพัฒนาออกเป็น ๔ แนวทาง ดังนี้

แนวทางการพัฒนาที่ ๑ นโยบายการบูรณาการฐานข้อมูลด้านความมั่นคง
แนวทางการพัฒนาที่ ๒ การพัฒนาระบบฐานข้อมูลด้านความมั่นคง
แนวทางการพัฒนาที่ ๓ การดำเนินงานด้านเทคนิคเพื่อบูรณาการข้อมูลระหว่างหน่วยงาน
แนวทางการพัฒนาที่ ๔ การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง

การดำเนินการตามแนวทางดังกล่าว ได้ให้ความสำคัญกับการจัดทำ Big Data ด้านความมั่นคง ซึ่งมุ่งเน้น การพัฒนาโครงสร้างพื้นฐานการจัดเก็บและประมวลผลหน่วยงานที่เกี่ยวข้องที่เหมาะสม การพัฒนาระบบสารสนเทศ เพื่อบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูลสำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ การพัฒนาระบบรายการข้อมูลภาครัฐ และการจัดทำระบบวิเคราะห์และจัดทำรายงาน ภายใต้กรอบ แนวคิดของการให้บริการข้อมูลภาครัฐ ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดขึ้น โดยมี กอ.รมน. เป็นหน่วยงานกลางทำหน้า ที่เป็น ศูนย์กลางข้อมูลด้านความมั่นคง (Data Center) ซึ่งรับผิดชอบการประสานและบูรณาการข้อมูล ตลอด จนเชื่อมโยงแลกเปลี่ยนข้อมูลกับหน่วยงานที่เกี่ยวข้อง เพื่อนำข้อมูลเสนอสภาความมั่นคงแห่งชาติ

ในส่วนของการดำเนินงานในการพัฒนาระบบ Big Data ด้านความมั่นคง เพื่อรองรับแนวทางการพัฒนาตามที่กำหนดใน แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ควรต้องมีการพัฒนาใน ๔ ระบบ ไปพร้อม ๆ กัน เพื่อให้สามารถรองรับงานในอนาคตได้อย่างอ่อนตัว และมีการพัฒนาทั้งระบบแบบยั่งยืน ซึ่งประกอบด้วย

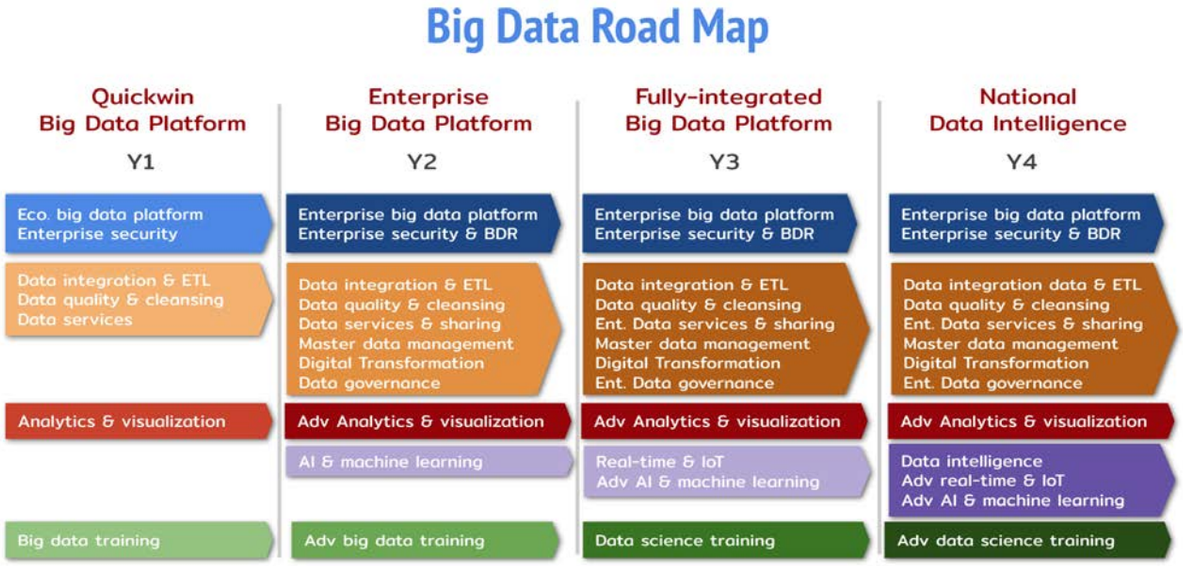
๑) ระบบบิ๊กดาต้าแพลตฟอร์ม (Big data platform) เป็นโครงสร้างพื้นฐานในด้านฮาร์ดแวร์และซอฟท์แวร์ รวมทั้งระบบรักษาความปลอดภัย สำหรับเป็นเครื่องมือในการจัดเก็บและประมวลผลข้อมูลขนาดใหญ่ ซึ่งจะเป็นโครงสร้างพื้นฐานสำหรับสนับสนุนงานในระบบอื่นๆ ทั้งระบบบริหารจัดการข้อมูล (Data management system) และระบบวิเคราะห์และทำรายงาน (Data analytics and visualization)

๒) ระบบบริหารจัดการข้อมูล (Data management system) เป็นเครื่องมือช่วยให้การบริหารจัดการกับข้อมูลขนาดใหญ่ ให้มีการจัดเก็บอย่างมีคุณภาพ มีระบบบริหารจัดการบัญชีข้อมูล (Data catalog managment) และระบบธรรมาภิบาลข้อมูล (Data governance system) เพื่อให้ข้อมูลมีความพร้อมสำหรับนำไปใช้ในการวิเคราะห์และทำรายงานได้อย่างถูกต้อง และเป็นไปตามมาตรฐานสากล

๓) ระบบวิเคราะห์ข้อมูล (Data analytics and visualization system) เป็นเครื่องมือสำหรับนักวิเคราะห์ข้อมูลหรือนักวิทยาศาสตร์ข้อมูล ให้สามารถวิเคราะห์ข้อมูลและทำรายงานแบบ dashboard หรือ mobile application เพื่อสนับสนุนผู้ใช้งานในระดับต่างๆ

๔) ระบบการฝึกอบรบมบุคลากรด้านบิ๊กดาต้า (Big data training) ให้บุคลากรด้านความมั่งคงทุกระดับ มีความรู้และทักษะในการทำงานด้านบิ๊กดาต้า รวมทั้งสามารถพัฒนาต่อยอดระบบได้อย่างยั่งยืน

จากการประเมินในขั้นต้น การพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง ซึ่งครอบคลุมงานทั้ง ๔ ระบบดังกล่าว เป็นงานที่ต้องกระทำโดยต่อเนื่อง เป็นระยะเวลาไม่น้อยกว่าสี่ปี ระบบจึงจะมีความพร้อมที่จะนำไปสู่การให้บริการข้อมูลอัจฉริยะในด้านความมั่งคงแห่งชาติได้อย่างเต็มรูปแบบ โดยในระยะที่ ๑ จะเริ่มต้นพัฒนาทั้ง ๔ ระบบไปพร้อมกัน โดยมุ่งเน้นการพัฒนาโครงสร้างพื้นฐาน และการพัฒนาระบบนำร่องที่เห็นผลในเวลาอันสั้น (Quickwin) ในระยะที่ ๒ จะยกระดับของบิ๊กดาต้าแพลตฟอร์มให้เป็นระดับองค์กร (Enterprise Platform) และเพิ่มระบบสำรอง รวมทั้งเพิ่มขีดความสามารถในการวิเคราะห์ข้อมูลชั้นสูง โดยเริ่มนำระบบ AI และ Machine Learning มาช่วยในการวิเคราะห์ข้อมูล ในระยะที่ ๓ จะมุ่งไปสู่การเชื่อมโยงและแลกเปลี่ยนข้อมูลโดยสมบูรณ์ (Fully-Integrated Platform) โดยมีการใช้ระบบ AI และ Machine Learning สนับสนุนการวิเคราะห์ข้อมูล สำหรับในระยะที่ ๔ จะเป็นการพัฒนาในทุกด้านโดยสมบูรณ์ รองรับการเป็นศูนย์บริการข้อมูลอัจฉริยะด้านความมั่งคงแห่งชาติ (National Data Intelligence)



แผนการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง (ระยะเวลา ๔ ปี)

การพัฒนาระบบบิ๊กดาต้าด้านความมั่นคงในปีที่ ๑

๑) ระบบบิ๊กดาต้าแพลตฟอร์ม มุ่งเน้นการพัฒนาระบบบิ๊กดาต้าแพลตฟอร์มพร้อมบริการพื้นฐานและระบบรักษาความปลอดภัยระดับองค์กร

๒) ระบบบริหารจัดการข้อมูล พัฒนาระบบการนำเข้าและเชื่อมโยงข้อมูล (Data integration) จากภายนอกมาจัดเก็บในบิ๊กดาต้าแพลตฟอร์ม การตรวจสอบคุณภาพข้อมูล (Data quality) การทำความสะอาดข้อมูล (Data cleansing) และการให้บริการข้อมูล (Data services) แก่หน่วยงานที่เกี่ยวข้อง

๓) ระบบวิเคราะห์ข้อมูล มุ่งเน้นการวิเคราะห์ข้อมูลเชิงพรรณนา (Descriptive Analytics) และการทำรายงานแบบแผนภาพ รวมทั้งการวิเคราะห์แนวโน้ม (Predicive Analytics) ซึ่งในปีนี้จะวิเคราะห์โจทย์

นำร่องจำนวนสามโจทย์ ได้แก่ ระบบวิเคราะห์และรายงานสถานการณ์จังหวัดชายแดนภาคใต้ ระบบวิเคราะห์ติดตามอาชญากรรมข้ามชาติและการก่อการร้าย และระบบวิเคราะห์สถานการณ์ป้องกันและแก้ไขปัญหาน้ำท่วม

๔) การฝึกอบรมบุคลากร เน้นการให้ความรู้พื้นฐานด้านบิ๊กดาต้า การใช้งานแพลตฟอร์ม การบริการจัดการข้อมูลเบื้องต้น การวิเคราะห์และทำรายงานเบื้องต้น และบิ๊กดาต้าสำหรับผู้บริหารระดับสูง

การพัฒนาระบบบิ๊กดาต้าด้านความมั่นคงใน ปีที่ ๒

๑) ระบบบิ๊กดาต้าแพลตฟอร์ม จะยกระดับของบิ๊กดาต้าแพลตฟอร์มให้เป็นระดับองค์กร รองรับการนำเข้าข้อมูลแบบ Real-time รวมทั้งเพิ่มระบบบิ๊กดาต้าแพลตฟอร์มสำรอง (DR-site) เพื่อให้ระบบงานสามารถทำงานได้อย่างต่อเนื่องแม้ระบบบิ๊กดาต้าแพลตฟอร์มหลักจะมีปัญหาข้อขัดข้อง

๒) ระบบบริหารจัดการข้อมูล จะเพิ่มบริการที่หลากหลายมากขึ้น เช่น การทำ Digital Transformation การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานผ่านบริการข้อมูล (Data Service) การกำกับดูแลการใช้ข้อมูลในองค์กรหรือธรรมมาภิบาลข้อมูล (Data Governance) และการบริหารจัดการข้อมูลหลักหรือข้อมูลต้นทาง (Master Data Management)

๓) ระบบวิเคราะห์ข้อมูล จะยกระดับความซับซ้อนของการวิเคราะห์ข้อมูลให้เป็นระดับสูง (Advanced Analytics and Visualization) รวมทั้งเริ่มมีการนำปัญญาประดิษฐ์หรือ AI และ Machine Learning เข้ามาใช้ในการเรียนรู้และทำนายผลการวิเคราะห์

๔) การฝึกอบรมบุคลากร จะเพิ่มระดับของเนื้อหาในหลักสูตรให้เป็นระดับสูง (Advanced big data training) เพื่อให้สอดคล้องกับระบบที่พัฒนาข้างต้นทั้งสามส่วน

การพัฒนาระบบบิ๊กดาต้าด้านความมั่นคงในปีที่ ๓

๑) ระบบบิ๊กดาต้าแพลตฟอร์ม จะเน้นการเชื่อมโยงและแลกเปลี่ยนข้อมูลโดยสมบูรณ์ (Fully-integrated Big Data Platform) ระหว่างหน่วยงานความมั่นคงกับหน่วยงานภายนอกอื่นๆ โดยส่วนของแพลตฟอร์มจะยังคงเป็นระบบเดิมที่พัฒนามาจากปีที่สองที่เป็นแพลตฟอร์มระดับองค์กร

๒) ระบบบริหารจัดการข้อมูล จะเป็นส่วนที่ได้รับพัฒนาให้เป็นระดับสูงสุดในปีนี้ เป็นระดับองค์กร หรือ Enterprise data management โดยยกระดับส่วนของการบริการและแลกเปลี่ยนข้อมูลเป็น Enterprise data services and sharing และยกระดับส่วนธรรมาภิบาลข้อมูลเป็น Enterprise data governance โดยบริการส่วนอื่นยังคงมีครบเหมือนเดิม

๓) ระบบวิเคราะห์ข้อมูล จะยังคงพัฒนาต่อในโจทย์ด้านอื่นๆ ต่อเนื่องจากปีที่ ๒ โดยใช้ฟังก์ชันในการวิเคราะห์ระดับสูงเช่นเดียวกับปีที่ผ่านมา แต่จะเพิ่มการนำเข้าข้อมูลแบบ real-time และ IoT เพื่อรองรับข้อมูลที่มาจากระบบอัตโนมัติในอนาคต รวมทั้งการใช้ AI และ Machine learning ทำโมเดลในการวิเคราะห์และเรียนระดับสูง

๔) การฝึกอบรมบุคลากร จะเพิ่มหลักสูตรการพัฒนานักวิทยาศาสตร์ข้อมูล (Data scientist) ที่มีความ รู้และทักษะสูงกว่านักวิเคราะห์ข้อมูล (Data analyst) ทั่วไป เช่น การใช้ AI และ machine learning ในการพัฒนาโมเดลหรือแอปพลิเคชันด้วยตนเองได้

การพัฒนาระบบบิ๊กดาต้าด้านความมั่นคงในปีที่ ๔

๑) ระบบบิ๊กดาต้าแพลตฟอร์ม จะได้รับการปรับปรุงให้ทันสมัย รวมทั้งจัดให้มีการบำรุงรักษาให้ระบบสามารถใช้งานได้อย่างต่อเนื่อง

๒) ระบบบริหารจัดการข้อมูล ที่ได้รับพัฒนาถึงระดับองค์กรในปีที่ ๓ จะได้รับการบำรุงรักษาให้ระบบสามารถใช้งานได้อย่างต่อเนื่อง

๓) ระบบวิเคราะห์ข้อมูล จะนำเทคโนโลยี AI และ Machine learning เข้ามาใช้ในการวิเคราะห์ข้อมูล ให้เป็นระบบ Data intelligence ด้านความมั่นคง รวมทั้งนำข้อมูลแบบ real-time และ IoT เข้ามาใช้โดยส่วนของ และ ในปีก่อนจะถูกนำมาใช้อย่างต่อเนื่อง

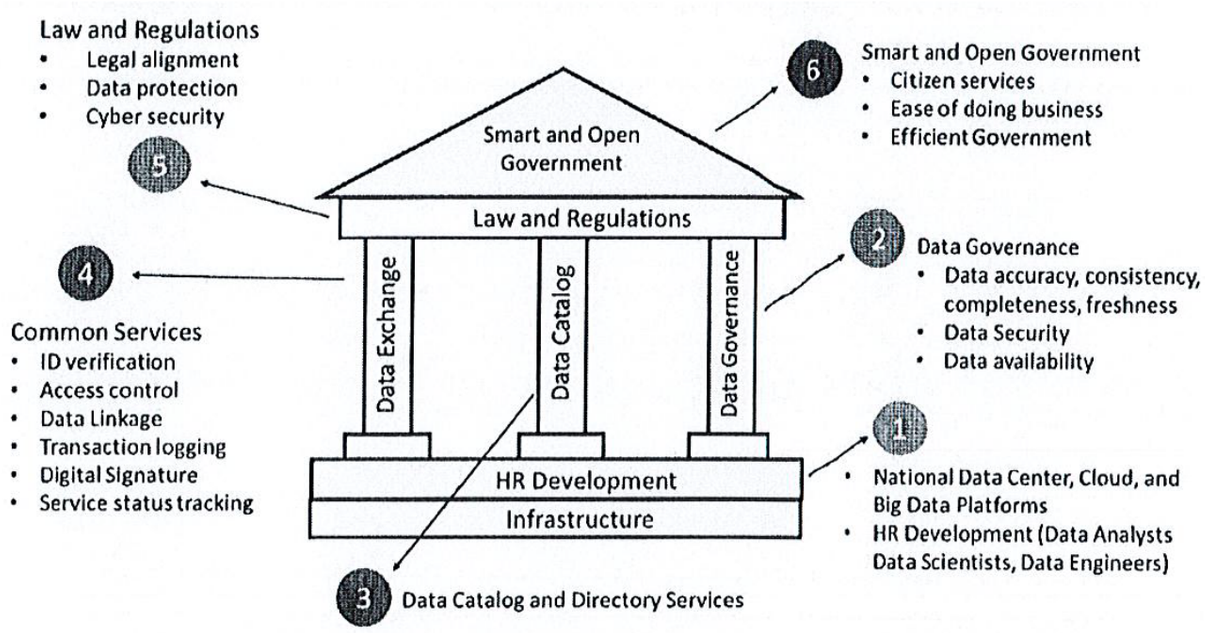
๔) การฝึกอบรมบุคลากร เพิ่มระดับการฝึกอบรมนักวิทยาศาสตร์ข้อมูลระดับสูง (Advanced data science training) รายละเอียดในการพัฒนาโครงการตามแผนแม่บทแต่ละปีจะอธิบายในบทต่อไปตามลำดับ

บทที่ ๑ บทนำ

๑.๑ ความเป็นมา

๑.๑.๑ แนวความคิดการนำระบบบิ๊กดาต้ามาให้บริการข้อมูลภาครัฐ

สิ่งจำเป็นและเป็นหัวใจต่อการการขับเคลื่อนเศรษฐกิจและสังคมของประเทศ ไปสู่ยุคไทยแลนด์ ๔.๐ คือ การที่ภาครัฐมีระบบการจัดเก็บและบริหารจัดการ รวมทั้งการใช้ประโยชน์จากข้อมูลดิจิทัลขนาดใหญ่อย่างเป็นรูปธรรม มีการรวบรวมข้อมูลที่หลากหลายจากทุกภาคส่วน และมีการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานอย่างเป็นระบบ เพื่อให้ประชาชนและหน่วยงานต่าง ๆ สามารถเข้าถึงข้อมูลเหล่านี้ได้โดยง่าย รวมทั้งมีระบบคลังข้อมูล (Data Warehouse) ขนาดใหญ่ของประเทศ บนโครงสร้างพื้นฐานทั้งทางด้านฮาร์ดแวร์และซอฟท์แวร์ ที่ทันสมัยมีประสิทธิภาพ และมีความปลอดภัย เพื่อใช้ในการจัดเก็บและประมวลผลข้อมูลขนาดใหญ่หรือที่เรียกว่า บิ๊กดาต้า (Big Data) รวมถึงการที่มีบุคลากรที่มีความรู้และประสบการณ์ ในการให้คำปรึกษาและฝึกอบรมบุคลากรภาครัฐ ให้สามารถบริการจัดการเทคโนโลยีด้านบิ๊กดาต้า และใช้ประโยชน์จากข้อมูลขนาดใหญ่ในส่วนที่ตนเองรับผิดชอบได้ ทั้งนี้การดำเนินการดังกล่าว จะอยู่บนพื้นฐานของกรอบแนวคิดการให้บริการข้อมูลภาครัฐ (Government Data Service Framework) ดังแสดงในแผนภาพที่ ๑



แผนภาพที่ ๑ แนวคิดของการให้บริการข้อมูลภาครัฐ (Government Data Service Framwork)
ที่มา: เอกสาร Big Data Framework กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรอบแนวคิดการให้บริการข้อมูลภาครัฐ (Government Data Service Framwork) ประกอบด้วยส่วนงานหลัก ๖ ส่วน ที่จะสร้างให้เกิดระบบนิเวศข้อมูล เพื่อสามารถใช้ประโยชน์ร่วมกันได้อย่างเป็นระบบ โดยทุกส่วนงาน ควรดำเนินการไปพร้อมๆ กัน ดังนี้

๑) การพัฒนาโครงสร้างพื้นฐานด้านฮาร์ดแวร์ ซอฟท์แวร์ และ Big Data Platform ที่เหมาะสม ทั้งในมิติด้านความต่อเนื่องของการบริการ การรักษาความปลอดภัย และการแลกเปลี่ยนเชื่อมโยงข้อมูลอย่างเป็นระบบ บนสถาปัตยกรรมโครงสร้างพื้นฐานแบบแบ่งปัน ที่ผู้รับบริการมองเสมือนว่าเป็นโครงสร้างเดียวที่ใช้ร่วมกัน รวมทั้งการพัฒนาบุคลากรภาครัฐให้มีศักยภาพ โดยเน้นการพัฒนานักวิทยาศาสตร์ข้อมูล และวิศวกรข้อมูล

๒) การส่งเสริมให้หน่วยงานของรัฐ สามารถจัดเก็บและกำกับดูแลข้อมูลในความรับผิดชอบ ให้มีความถูกต้อง สอดคล้องตรงกัน สมบูรณ์ ทันสมัย และอยู่ในสภาพที่พร้อมใช้งาน โดยมีการกำกับดูแลความปลอดภัยของข้อมูลตามชั้นความลับที่ได้มาตรฐาน

๓) การพัฒนาระบบรายการข้อมูลภาครัฐ (**Government Data Catalog**) โดยรวบรวมสรุปรายการโครงสร้างข้อมูล (Metadata) ของข้อมูลสำคัญ จากหน่วยงานภาครัฐทั้งหมด เพื่อจัดสร้างเป็นรายการข้อมูล (Data Catalog) เพื่อให้บริการสืบค้นข้อมูล เสมือนสมุดหน้าเหลือง (Yellow Pages)

๔) พัฒนาระบบสารสนเทศ เพื่อบริหารจัดการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ เพื่อใช้ในการวิเคราะห์ข้อมูลขนาดใหญ่ (**Big Data Analytics**) และการให้บริการประชาชน โดยมีบริการพื้นฐาน เช่น การยืนยันตัวตน การกำหนดสิทธิในการเข้าถึงข้อมูล การบริการส่งข้อมูลข้ามหน่วยงานผ่านระบบสารสนเทศ การบันทึกธุรกรรม (**Transaction**) การเข้าถึงข้อมูลเพื่อเป็นหลักฐาน และการบริการข้อมูลประเภทอื่น

๕) ศึกษากระบวนการทางกฎหมาย และกฎหมายต่างๆ ที่เกี่ยวข้อง เพื่อออกแบบแนวทางปฏิบัติที่เหมาะสม เพื่อเอื้อให้เกิดการใช้ประโยชน์ข้อมูล และการบูรณาการข้อมูลข้ามหน่วยงานได้อย่างเป็นรูปธรรม

๖) เป้าหมายระยะยาวของกรอบการวิเคราะห์ข้อมูลขนาดใหญ่ภาครัฐ คือ การที่กระทรวง รัฐวิสาหกิจ และส่วนราชการทุกแห่ง มีศักยภาพในการจัดเก็บและประมวลผลข้อมูลได้อย่างเป็นระบบ รวมทั้งสามารถเชื่อมโยงแลกเปลี่ยนข้อมูลและใช้ประโยชน์ข้อมูลขนาดใหญ่ ได้อย่างเป็นรูปธรรม

กรอบการกำกับดูแลข้อมูลภาครัฐในระดับหน่วยงาน จะประกอบด้วยองค์ประกอบต่างๆ ผนวกเข้าด้วยกัน ทั้งในด้านของนิยามและกฎที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ สรุปรายละเอียดตามแผนภาพที่ ๒

แผนภาพที่ ๒ กรอบการกำกับดูแลข้อมูลในระดับหน่วยงาน
ที่มา: เอกสาร กรอบการกำกับดูแลข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

แผนภาพที่ ๒ แสดงกรอบการกำกับดูแลข้อมูลในระดับหน่วยงาน ประกอบด้วย นิยามและกฎที่เกี่ยวข้องกับข้อมูล (**Definitions and Rules**) โครงสร้างการกำกับดูแลข้อมูล (**Data Governance Structure**) และกระบวนการกำกับดูแลข้อมูล (**Data Governance Processes**) โดยบุคคลต่างๆ ที่เกี่ยวข้องกับโครงสร้างการกำกับดูแลข้อมูล จะเป็นผู้กำหนดนิยามและกฎที่เกี่ยวข้องกับข้อมูล สำหรับใช้ในการสร้างการกำกับดูแลข้อมูล เพื่อให้สอดคล้องกับกระบวนการที่กำหนดไว้

๑.๑.๒ การบูรณาการข้อมูลและประยุกต์ใช้ระบบบิ๊กดาต้าด้านความมั่นคง

สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ในฐานะหน่วยงานภาครัฐ ที่รับผิดชอบกำกับดูแลด้านนโยบาย ความมั่นคงทั้งปวง และ กำกับดูแลการขับเคลื่อนยุทธศาสตร์ชาติด้านความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) ให้บังเกิดผลสำเร็จ อย่างเป็นรูปธรรมชัดเจนตามเป้าหมายที่กำหนด ได้เล็งเห็นความสำคัญของระบบบิ๊กดาต้า ที่สามารถนำมาประยุกต์ใช้ในการบูรณาการเชื่อมโยงข้อมูลด้านความมั่นคงระหว่างหน่วยงานต่างๆ จึงได้จัดทำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๓ - ๒๕๖๕) โดยมีเป้าหมายเพื่อพัฒนาระบบฐานข้อมูลด้านความมั่นคงให้มีความทันสมัย เพื่อใช้ประโยชน์ในการแก้ไขปัญหาความมั่นคงของประเทศ โดยเน้นบูรณาการเชื่อมโยงข้อมูลระหว่างหน่วยงาน และการให้ความสำคัญกับการจัดทำ Big Data Platform ด้านความมั่นคง ซึ่งประกอบด้วย การพัฒนาโครงสร้างพื้นฐานการจัดเก็บและประมวลผลหน่วยงานที่เหมาะสม การพัฒนาระบบสารสนเทศเพื่อบริการจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูลสำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ และการพัฒนาระบบรายการข้อมูลภาครัฐ (Governance Data Catalog) รวมทั้งการพัฒนาบุคลากรด้านความมั่นคง ให้มีขีดความสามารถในการบริหารจัดการและการใช้ประโยชน์ข้อมูลแบบองค์รวม

๑.๒ วัตถุประสงค์การพัฒนาระบบบิ๊กดาต้าเพื่อความมั่นคง

๑.๒.๑ เพื่อพัฒนาโครงสร้างพื้นฐานระบบการจัดเก็บและประมวลผลข้อมูลที่เหมาะสม โดยหน่วยงานที่เกี่ยวข้อง มีการเชื่อมโยงแลกเปลี่ยนข้อมูลอย่างเป็นระบบ ภายใต้การรักษาความปลอดภัยที่ได้มาตรฐาน และรองรับการให้บริการข้อมูลได้อย่างต่อเนื่อง บนพื้นฐานสถาปัตยกรรมแบบแบ่งปัน ที่ผู้รับบริการมองเสมือนว่าเป็นโครงสร้างเดียวที่ใช้ร่วมกัน

๑.๒.๒ เพื่อพัฒนาระบบสารสนเทศ เพื่อบริหารจัดการการเชื่อมโยง และแลกเปลี่ยนข้อมูล ด้านความมั่นคง สำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) โดยมีบริการพื้นฐาน เช่น การยืนยันตัวตน การกำหนดสิทธิ ในการเข้าถึงข้อมูล การให้บริการการ รับ-ส่ง ข้อมูล ระหว่างหน่วยงานผ่านระบบสารสนเทศ การบันทึกธุรกรรม (Transaction) การเข้าถึงและใช้ข้อมูลเพื่อเป็นหลักฐาน และการบริการข้อมูลประเภทอื่นๆ รวมทั้งการจัดทำรายการโครงสร้างข้อมูลด้านความมั่นคง และข้อมูลที่เกี่ยวข้องกับความมั่นคง

๑.๒.๓ เพื่อพัฒนาระบบสนับสนุนระบบวิเคราะห์ข้อมูลและรายงาน (Data analytics and visualization system) เพื่อใช้ในการติดตามสถานการณ์ การเฝ้าระวัง และการแจ้งเตือน ภัยความมั่นคงของชาติในทุกมิติ ครอบคลุมการวิเคราะห์หาสาเหตุ การวิเคราะห์เพื่อป้องกันเหตุ การวิเคราะห์ เพื่อสนับสนุนการตัดสินใจ โดยสามารถตอบสนองกลุ่มผู้ใช้งานในทุกระดับ ตั้งแต่ผู้บริหารระดับสูง นักวิเคราะห์ข้อมูล และเจ้าหน้าที่ที่เกี่ยวข้อง

๑.๒.๔ เพื่อพัฒนาบุคลากรด้านบิ๊กดาต้า (Big data training) ให้บุคลากรด้านความมั่งคงทุกระดับ มีความรู้และทักษะในการทำงานด้านบิ๊กดาต้าได้จริง และสามารถพัฒนาต่อยอดระบบที่มีอยู่ได้เองอย่างยั่งยืน

๑.๓ เป้าหมายในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง

๑.๓.๑ ระบบ Big Data Platform ด้านความมั่นคง ที่มีลักษณะเป็นดาต้าเซ็นเตอร์ติดตั้งบนระบบคลาวด์ บนพื้นฐานสถาปัตยกรรมแบบแบ่งปัน ที่ผู้รับบริการมองเสมือนว่าเป็นโครงสร้างเดียวที่ใช้ร่วมกัน และมีประสิทธิภาพในการรักษาความปลอดภัยสูง

๑.๓.๒ ระบบบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูลด้านความมั่นคง ที่มีการกำหนดระดับการ เข้าถึงข้อมูล ภายใต้ระบบการรักษาความปลอดภัยข้อมูลตามมาตรฐานระดับสากล มีการแลกเปลี่ยนข้อมูลที่เป็นระบบ สามารถการทำงานได้อย่างต่อเนื่องและมีประสิทธิภาพ รวมทั้งมีการจัดทำรายการข้อมูลด้านความมั่นคง และข้อมูลที่เกี่ยวข้องกับความมั่นคง ที่หน่วยงานที่เกี่ยวข้องสามารถสืบค้นได้ง่าย

๑.๓.๓ ระบบการสนับสนุนและช่วยเหลือ การรายงานสถานการณ์ความมั่นคงของชาติในทุกมิติ และครอบคลุมทุกๆ ด้าน ทั้งด้านการวิเคราะห์สาเหตุ การวางแผนและตัดสินใจ โดยตอบสนองทุกกลุ่มผู้ใช้งาน ไม่ว่าจะเป็นในระดับผู้บริหาร เจ้าหน้าที่ที่ปฏิบัติงานทั้งในและนอกสำนักงาน รวมถึงมีการพัฒนาระบบข้อมูลแจ้งเตือนสถานะที่จำเป็นรอบด้าน แบบ Real-time

๑.๓.๔ บุคลากรภาครัฐที่เกี่ยวข้องในทุกระดับมีศักยภาพในการประยุกต์ใช้ระบบบิ๊กดาต้า ในการป้องกัน และแก้ไขปัญหาด้านความมั่นคง ได้อย่างมีประสิทธิภาพ

๑.๔ ตัวชี้วัดความสำเร็จในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง

๑.๔.๑ ระดับความสำเร็จการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคงที่เป็นแพลตฟอร์มบิ๊กดาต้าบนคลาวด์ที่มีประสิทธิภาพ เพื่อการบูรณาการการทำงานระหว่างหน่วยงาน

๑.๔.๒ ระดับความสำเร็จการมีกลไกในการแลกเปลี่ยนเชื่อมโยงข้อมูล ระหว่างหน่วยงานด้านความมั่นคงและ/หรือกับหน่วยงานที่สนับสนุนภารกิจด้านความมั่นคง ในระบบบิ๊กดาต้าด้านความมั่นคง ให้มีประสิทธิภาพเพิ่มมากขึ้น

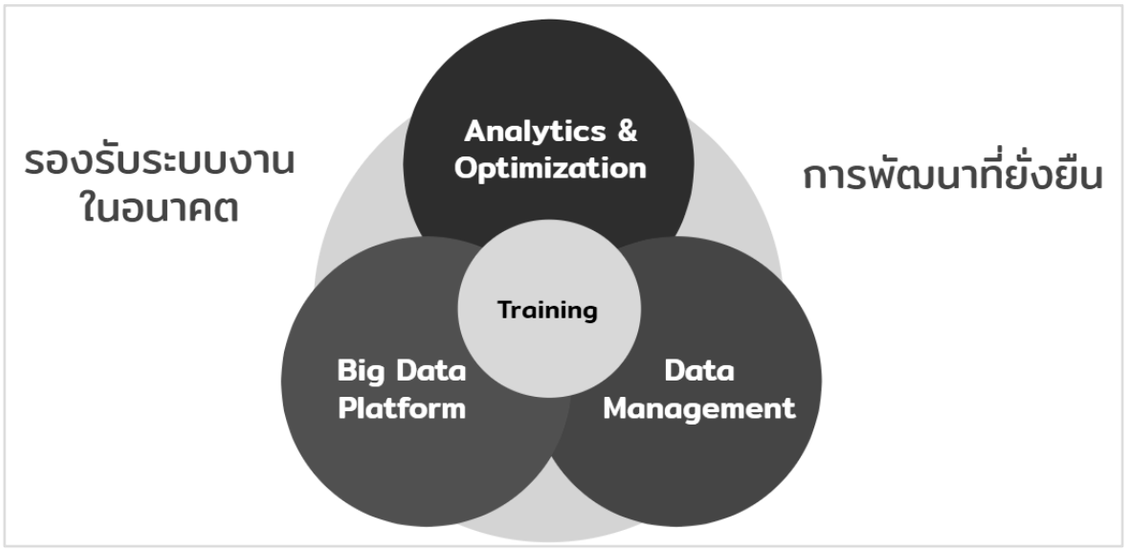
๑.๔.๓ ระดับความสำเร็จการบริหารจัดการข้อมูลด้านความมั่นคง ในระบบบิ๊กดาต้าด้านความมั่นคง เพื่อประกอบการเสนอแนะนโยบาย/แผนและแนวทาง ในการป้องกันและแก้ไขปัญหาความมั่นคง

๑.๔.๔ ระดับความสำเร็จในการพัฒนาบุคลากรด้านความมั่นคงให้ได้ใช้เทคโนโลยีสารสนเทศที่ทันสมัยในการปฏิบัติงาน และนำข้อมูลขนาดใหญ่มาใช้ให้เกิดประโยชน์สูงสุดในการป้องกันและแก้ไขปัญหาด้านความมั่นคงของประเทศ

บทที่ ๒ แนวทางการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง

๒.๑ แนวคิดในการพัฒนาระบบบิ๊กดาต้า

แนวคิดในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง (Big Data Concept) เพื่อให้สามารถรองรับงานในอนาคตได้หลากหลายและมีความยั่งยืน จำเป็นต้องมีการพัฒนาองค์ประกอบหลัก ๔ ด้าน ไปพร้อมๆ กัน ดังแผนภาพที่ ๓



แผนภาพที่ ๓ องค์ประกอบหลักในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง

องค์ประกอบหลักในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง ๔ ด้าน ประกอบด้วย

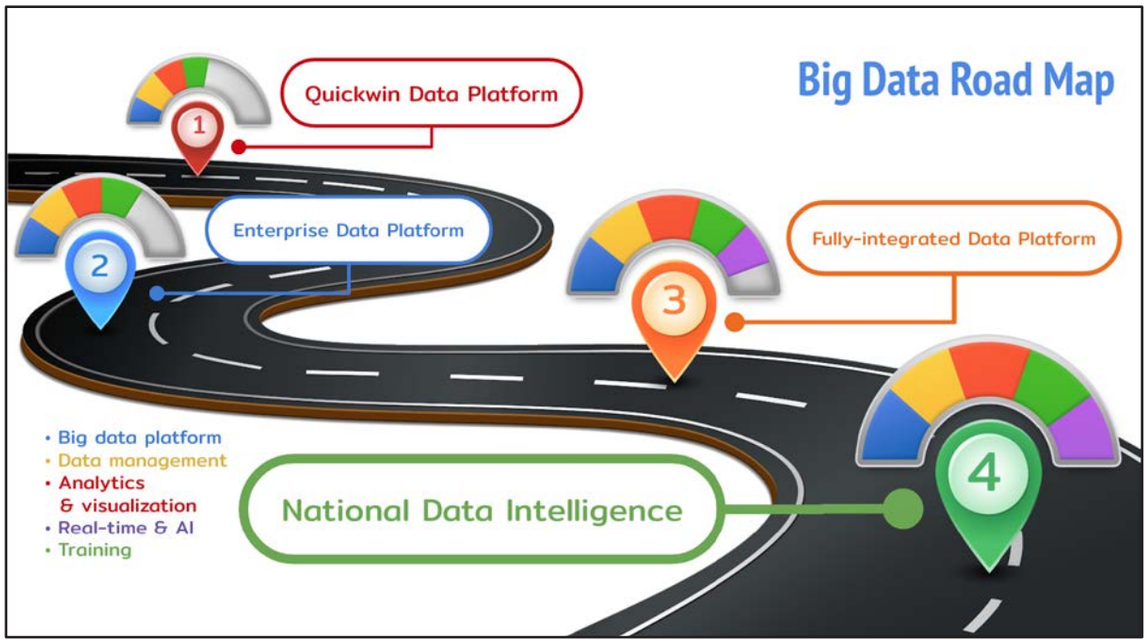
๑) **บิ๊กดาต้าแพลตฟอร์ม (Big data platform)** เป็นเครื่องมือในการจัดเก็บและประมวลผลข้อมูลขนาดใหญ่ และช่วยสนับสนุนงานในระบบอื่นๆ ทั้งระบบบริหารจัดการข้อมูล (Data management system) และระบบวิเคราะห์และทำรายงาน (Data analytics and visualization) ให้มีประสิทธิภาพ

๒) **ระบบบริหารจัดการข้อมูล (Data management system)** เป็นเครื่องมือช่วยให้การบริหารจัดการข้อมูลขนาดใหญ่อย่างมีคุณภาพ มีระบบบริหารจัดการบัญชีข้อมูล (Data catalog management) และระบบธรรมาภิบาลข้อมูล (Data governance system) เพื่อให้ข้อมูลมีความพร้อมสำหรับนำไปใช้ในการวิเคราะห์และทำรายงานได้อย่างถูกต้องและเป็นไปตามมาตรฐานสากล

๓) **ระบบวิเคราะห์ข้อมูลและทำรายงาน (Data analytics and visualization system)** เป็นเครื่องมือสำหรับช่วยนักวิเคราะห์ข้อมูลหรือนักวิทยาศาสตร์ข้อมูล เพื่อให้สามารถวิเคราะห์ข้อมูลและจัดทำรายงาน ในรูปแบบ dashboard หรือ mobile application สนับสนุนผู้บริหารระดับสูง ในการนำผลการวิเคราะห์ไปใช้ในการวางแผนและตัดสินใจได้อย่างรวดเร็วและแม่นยำ

๔) **การฝึกอบรมบุคลากรด้านบิ๊กดาต้า (Big data training)** ให้บุคลากรด้านความมั่งคงทุกระดับมีความรู้และทักษะในการทำงานด้านบิ๊กดาต้าได้จริง และสามารถพัฒนาต่อยอดระบบที่มีอยู่ได้เองอย่างยั่งยืน ด้วยการฝึกอบรมเชิงปฏิบัติการ (Training workshop) กับงานและข้อมูลจริง โดยผู้เชี่ยวชาญด้านบิ๊กดาต้าในแต่ละสาขา

จากการประเมินในขั้นต้น การพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง ซึ่งครอบคลุมงานทั้ง ๔ ด้าน ดังกล่าว เป็นงานที่ต้องกระทำโดยต่อเนื่อง เป็นระยะเวลาไม่น้อยกว่า ๔ ปี ระบบจึงจะมีความพร้อมที่จะนำไปสู่การให้บริการข้อมูลอัจฉริยะในด้านความมั่งคง (Security Data Intelligence) ได้อย่างเต็มรูปแบบ ทั้งนี้ได้มีการกำหนดแนวทางในการวางแผนแม่บทหรือแผนระยะยาว (Road map) ในการพัฒนาระบบไว้ในห้วงระยะเวลา ๔ ปี ดังแสดงในแผนภาพที่ ๔



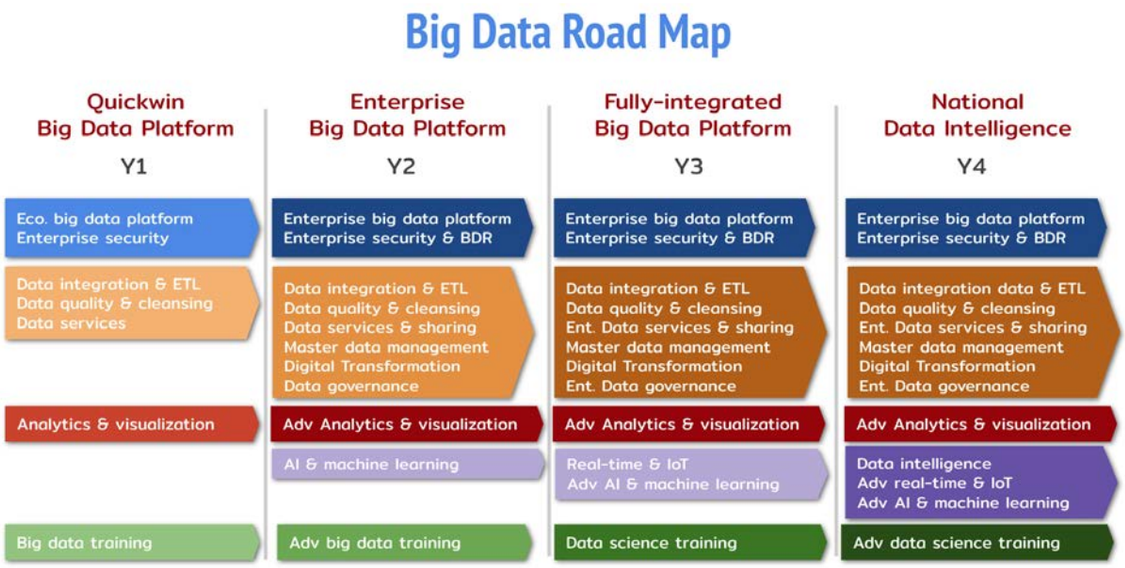
แผนภาพที่ ๔ แผนระยะยาวในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง

จากแผนภาพที่ ๔ ซึ่งแสดงกรอบแนวทางในการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง (Security big data road map) โดยเริ่มจากการพัฒนาแพลตฟอร์มพื้นฐาน (Quickwin data platform) ในปีแรก เพื่อเน้นการสร้างโครงสร้างพื้นฐานทั้ง ๔ ด้าน โดยเฉพาะในส่วนของแพลตฟอร์มที่มีประสิทธิภาพและความปลอดภัยสูง จากนั้นในปีที่สองจะยกระดับส่วนของการบริหารจัดการข้อมูลให้เป็น แพลตฟอร์มระดับองค์กร (Enterprise data platform) ที่สามารถบริหารจัดการข้อมูลในระดับประเทศได้ครบถ้วน เป็นไปตามมาตรฐานสากล และเพิ่มเติมขีดความสามารถด้านการวิเคราะห์ข้อมูล (Data Analytics) สำหรับปีที่สามจะเป็นการพัฒนาต่อยอดจากระบบบริหารจัดการข้อมูล นำไปสู่แพลตฟอร์มการเชื่อมโยงข้อมูลแบบสมบูรณ์ (Fully-integrated data platform) โดยเน้นการเชื่อมโยงข้อมูล (Data integration) จากข้อมูลที่หลากหลาย โดยเฉพาะการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานด้านความมั่นคงที่ครบถ้วน และในปีที่สี่จะเป็นการนำข้อมูล

ที่มีการเชื่อมโยงและบูรณาการ ไปวิเคราะห์เชิงลึกด้วยเทคโนโลยีปัญญาประดิษฐ์หรือ AI และ Machine Learning ซึ่งเป็นการพัฒนาโมเดลต้นแบบให้มีการเรียนรู้และวิเคราะห์ด้วยตนเอง และนำไปสู่การให้บริการข้อมูลอัจฉริยะ (Data intelligence) ได้อย่างแท้จริง

๒.๒ แผนการพัฒนาระบบบิ๊กดาต้าด้านความมั่นคง

เพื่ออธิบายกรอบแนวทางในการพัฒนาระบบบิ๊กดาต้าความมั่นคง ตามที่กล่าวมาข้างต้น จึงได้กำหนดรายละเอียดแนวทางแผนแม่บทในการพัฒนาบิ๊กดาต้าด้านความมั่นคงในแต่ละปี ดังแสดงในแผนภาพที่ ๕



แผนภาพที่ ๕ องค์ประกอบในการพัฒนาระบบตามแผนแม่บทบิ๊กดาต้าด้านความมั่นคง

แผนภาพที่ ๕ แสดงให้เห็นองค์ประกอบในการพัฒนาระบบแต่ละปี โดยแยกการพัฒนาออกเป็น ๕ ส่วน ได้แก่ การพัฒนาบิ๊กดาต้าแพลตฟอร์ม การพัฒนาระบบบริหารจัดการข้อมูล การพัฒนาระบบวิเคราะห์และทำรายงาน การพัฒนาระบบอัจฉริยะ และการฝึกอบรมบุคลากรด้านบิ๊กดาต้า โดยแผนแม่บทได้ออกแบบให้มีการพัฒนาองค์ประกอบเหล่านี้อย่างต่อเนื่องตั้งแต่ปีที่หนึ่งจนถึงปีที่สี่ สรุปได้ดังนี้

ปีที่หนึ่งจะเน้นการพัฒนาระบบพื้นฐานทั้งสี่ด้าน ได้แก่ ระบบบิ๊กดาต้าแพลตฟอร์มพร้อมบริการพื้นฐาน (Big data platform and foundation services) และระบบรักษาความปลอดภัยระดับองค์กร (Enterprise security) เพื่อเน้นประสิทธิภาพและความปลอดภัยของระบบ ระบบบริหารจัดการข้อมูล (Data management system) โดยมีบริการนำเข้าและเชื่อมโยงข้อมูล (Data integration) จากภายนอกมาจัดเก็บในบิ๊กดาต้าแพลตฟอร์ม การตรวจสอบคุณภาพข้อมูล (Data quality) การทำความสะอาดข้อมูล (Data cleansing) และการให้บริการข้อมูล (Data services) แก่หน่วยงานที่เกี่ยวข้อง ระบบวิเคราะห์ข้อมูลและการทำรายงานแบบแผนภาพ (Data analytics and visualization) รวมทั้งระบบแจ้งเตือนภัย ซึ่งในปีนี้จะวิเคราะห์โจทย์ด้านความมั่นคงจำนวนสามโจทย์ ได้แก่ (๑) ระบบวิเคราะห์และรายงานสถานการณ์สามจังหวัดชายแดนภาคใต้ (๒) ระบบวิเคราะห์ติดตามอาชญากรรมข้ามชาติและการก่อการร้าย (๓) ระบบวิเคราะห์

สถานการณ์ ป้องกันและแก้ไขปัญหาน้ำท่วม รวมทั้งการฝึกอบรมบุคลากรด้านบิ๊กดาต้า (Big data training) ซึ่งเน้นการให้ความรู้พื้นฐานด้านบิ๊กดาต้า การใช้งานแพลตฟอร์ม การบริการจัดการข้อมูลเบื้องต้น การวิเคราะห์และทำรายงานเบื้องต้น และบิ๊กดาต้าสำหรับผู้บริหารระดับสูง

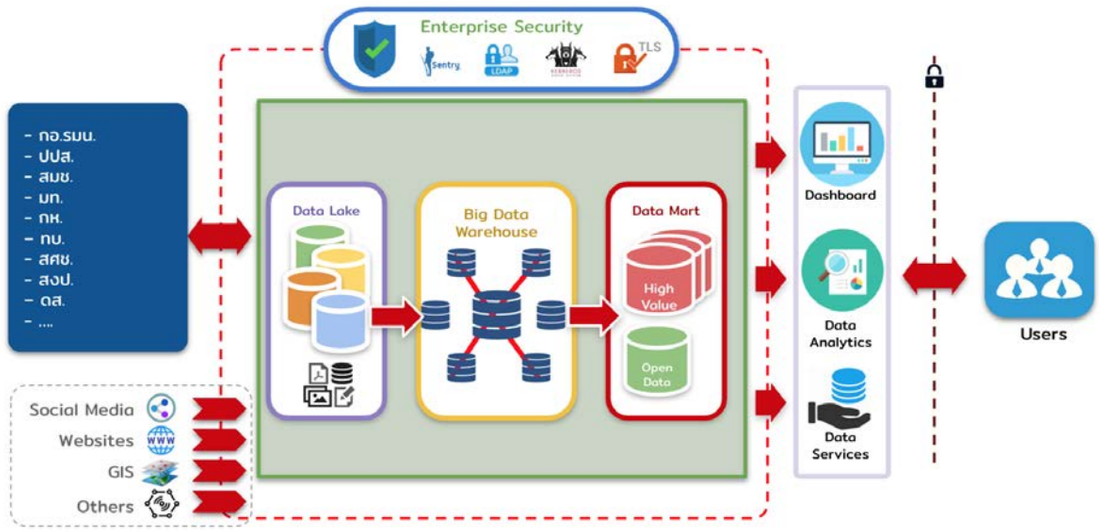
ปีที่สองจะเน้นการยกระดับของบิ๊กดาต้าแพลตฟอร์มให้เป็นระดับองค์กร (Enterprise Big Data Platform) สามารถรองรับการนำเข้าข้อมูลแบบ real-time ได้อย่างมีประสิทธิภาพ รวมทั้งเพิ่มบิ๊กดาต้าแพลตฟอร์มสำรอง (DR-site) เพื่อให้ระบบงานสามารถทำงานได้อย่างต่อเนื่องแม้บิ๊กดาต้าแพลตฟอร์มหลักจะมีปัญหาข้อขัดข้อง หรือข้อมูลหลักสูญหาย ในส่วนของระบบบริหารจัดการข้อมูลจะเพิ่มบริการที่หลากหลายมากขึ้น ได้แก่ การทำ Digital Transformation การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานผ่านบริการข้อมูล (Data service) การกำกับดูแลการใช้ข้อมูลในองค์กรหรือธรรมาภิบาลข้อมูล (Data governance) และการบริหารจัดการข้อมูลหลักหรือข้อมูลต้นทาง (Master data management) สำหรับการวิเคราะห์ข้อมูลและทำรายงาน จะยกระดับความซับซ้อนของการวิเคราะห์ข้อมูลให้เป็นระดับสูง (Advanced analytics and visualization) รวมทั้งเริ่มมีการนำปัญญาประดิษฐ์หรือ AI และ Machine learning เข้ามาใช้ในการเรียนรู้และทำนายผลการวิเคราะห์และส่วนสุดท้ายคือการฝึกอบรมบุคลากร จะเพิ่มระดับของเนื้อหาในหลักสูตรให้เป็นระดับสูง (Advanced big data training) เพื่อให้สอดคล้องกับระบบที่เราพัฒนาข้างต้นทั้งสามส่วนด้วย

ปีที่สามจะเน้นการเชื่อมโยงและแลกเปลี่ยนข้อมูลโดยสมบูรณ์ (Fully-integrated Big Data Platform) ระหว่างหน่วยงานความมั่นคงกับหน่วยงานภายนอกอื่นๆ โดยส่วนของแพลตฟอร์มจะยังคงเป็นระบบเดิมที่พัฒนามาจากปีที่สองที่เป็นแพลตฟอร์มระดับองค์กร ส่วนการบริหารจัดการข้อมูลจะเป็นส่วนที่พัฒนาให้เป็นระดับสูงสุดในปีนี้เป็นระดับองค์กรหรือ Enterprise data management โดยยกระดับส่วนของการบริการและแลกเปลี่ยนข้อมูลเป็น Enterprise data services and sharing และยกระดับส่วนธรรมาภิบาลข้อมูลเป็น Enterprise data governance โดยบริการส่วนอื่นยังคงมีครบเหมือนเดิม สำหรับการวิเคราะห์และทำรายงานในปีนี้จะยังคงพัฒนาต่อในโจทย์ด้านอื่นๆ ที่ยังไม่ได้ทำหรือทำไม่สมบูรณ์ โดยใช้ฟังก์ชันในการวิเคราะห์ระดับสูงเช่นเดียวกับปีที่ผ่านมา แต่จะเพิ่มการนำเข้าข้อมูลแบบ real-time และ IoT เพื่อรองรับข้อมูลที่มาจากระบบอัตโนมัติในอนาคต รวมทั้งการใช้ AI และ Machine learning ทำโมเดลในการวิเคราะห์และเรียนระดับสูง ส่วนสุดท้ายในการฝึกอบรมบุคลากร จะเพิ่มหลักสูตรการพัฒนานักวิทยาศาสตร์ข้อมูล (Data scientist) ที่มีความรู้และทักษะสูงกว่านักวิเคราะห์ข้อมูล (Data analyst) ทั่วไป เช่น การใช้ AI และ machine learning มาทำโมเดลหรือการพัฒนาแอปพลิเคชันด้วยตนเองได้

ปีที่สี่จะนำเทคโนโลยี AI และ Machine learning เข้ามาใช้ในการวิเคราะห์ข้อมูลอย่างเต็มรูปแบบให้เป็นระบบ Data intelligence ด้านความมั่นคง รวมทั้งนำข้อมูลแบบ real-time และ IoT เข้ามาใช้อย่างเต็มรูปแบบ โดยส่วนของบิ๊กดาต้าแพลตฟอร์ม และระบบบริหารจัดการข้อมูลที่ได้พัฒนาถึงระดับองค์กร ในปีก่อนจะถูกนำมาใช้อย่างต่อเนื่อง รวมทั้งการเพิ่มระดับการฝึกอบรมนักวิทยาศาสตร์ข้อมูลระดับสูง (Advanced data science training) รายละเอียดในการพัฒนาโครงการตามแผนแม่บทแต่ละปีจะอธิบายในบทต่อไปตามลำดับ

บทที่ ๓ การพัฒนาบิ๊กดาต้าด้านความมั่นคงระยะที่ ๑ ปีที่ ๑

โครงการปีที่ ๑ เป็นการพัฒนาบิ๊กดาต้าแพลตฟอร์มพื้นฐาน (Quickwin Big Data Platform) โดยสร้างระบบพื้นฐานของบิ๊กดาต้าทั้ง ๔ ด้าน ได้แก่ ระบบบิ๊กดาต้าแพลตฟอร์มพร้อมระบบรักษาความปลอดภัย ระบบบริหารจัดการข้อมูล ระบบวิเคราะห์ข้อมูลและทำรายงาน และการฝึกอบรมบุคลากร โดยปีนี้จะเน้นในด้านความปลอดภัยข้อมูลให้เป็นระดับองค์กร (Enterprise security) เป็นหลัก ในส่วนของโครงสร้างระบบจะเป็นดังแผนภาพที่ ๖



แผนภาพที่ ๖ สถาปัตยกรรมบิ๊กดาต้าแพลตฟอร์มพื้นฐานระยะที่ ๑ ปีที่ ๑

แผนภาพที่ ๖ แสดงสถาปัตยกรรมบิ๊กดาต้าแพลตฟอร์มพื้นฐาน (Quickwin Big Data Platform) ระยะที่ ๑ ปีที่ ๑ ซึ่งเน้นการวางรากฐานของระบบทั้ง ๔ ด้าน โดยเฉพาะส่วนของระบบรักษาความปลอดภัย ที่เป็น Enterprise security หรือระบบรักษาความปลอดภัยระดับองค์กรทำให้แพลตฟอร์ม มีทั้งประสิทธิภาพและความปลอดภัยในระดับสูง โดยข้อมูลที่เชื่อมโยงระหว่างหน่วยงานความมั่นคงต่างๆ และข้อมูลจากแหล่งข้อมูลทั่วไปจะถูกนำเข้ามาจัดเก็บในบิ๊กดาต้าแพลตฟอร์มที่ส่วนของทะเลสาบข้อมูล (Data lake) ก่อนจากนั้นข้อมูลในส่วนนี้จะถูกนำไปตรวจสอบคุณภาพและทำความสะอาด รวมทั้งแปลงให้อยู่ในรูปแบบที่นักวิเคราะห์ต้องการ ซึ่งจะถูกเก็บไว้ในคลังข้อมูล (Data warehouse) สำหรับส่วนสุดท้ายเรียกว่าตลาดข้อมูล (Data mart) จะเป็นชุดข้อมูลคุณภาพสูง ที่ถูกปรับปรุงให้มีประสิทธิภาพและเหมาะสมต่องานเฉพาะ ซึ่งจะถูกนำไปใช้ในการ วิเคราะห์ข้อมูล (Data analytics) การทำรายงานแบบแผนภาพ (Data visualization) หรือ Dashboard และการให้บริการข้อมูล (Data service) เป็นต้น ซึ่งข้อมูลที่ผ่านกระบวนการต่างๆ เหล่านี้ตั้งแต่ต้นจนจบ จะ ถูกควบคุมด้วยระบบรักษาความปลอดภัย ที่มีการยืนยันตัวบุคคล (Authentication) และการกำหนดสิทธิ ใน การเข้าถึงและการใช้งานข้อมูล (Authorization) รวมทั้งการเข้ารหัสข้อมูล (Data encryption) สำหรับราย ละเอียดของ โครงการระยะที่ ๑ มีดังนี้

๓.๑ วัตถุประสงค์โครงการ

๓.๑.๑ เพื่อสร้างและวางรากฐานที่เข้มแข็ง ของระบบบิ๊กดาต้าด้านความมั่นคง ให้เป็นไปตามมาตรฐานสากล รวมถึงการพัฒนาระบบให้มีความยืดหยุ่น สามารถรองรับการเปลี่ยนแปลงของเทคโนโลยีในอนาคตได้

๓.๑.๒ เพื่อนำระบบบิ๊กดาต้าเข้ามาสนับสนุนการปฏิบัติงานทางด้านความมั่นคง ในส่วนของการติดตามสถานการณ์และเฝ้าระวังภัยคุกคาม

๓.๑.๓ เพื่อให้ข้อมูลด้านความมั่นคงที่มีอยู่ ได้รับการบริหารจัดการที่ถูกต้อง เป็นระบบที่มีรูปแบบการจัดเก็บที่เป็นมาตรฐานกลาง ซึ่งรองรับการเข้าถึงในทุกรูปแบบ เช่น Web app และ Mobile app เป็นต้น พร้อมทั้งมีการรักษาความปลอดภัยข้อมูลระดับองค์กร (Enterprise Security)

๓.๑.๔ เพื่อสามารถนำข้อมูลที่มี มาสรุปออกมาในรูปแบบกราฟิกเชิงสถิติที่สามารถเข้าใจได้ง่าย

๓.๑.๕ เพื่อให้มีทรัพยากรที่สามารถนำมาสนับสนุน การพัฒนาบุคลากรของหน่วยงานด้านความมั่นคงในด้านการบริหารจัดการข้อมูลบิ๊กดาต้า

๓.๒ แผนการดำเนินการ

โครงการพัฒนาระบบบิ๊กดาต้าพื้นฐาน ระยะที่ ๑ ปีที่ ๑ มีแผนการดำเนินงาน ๑๒ เดือน ประกอบด้วยกิจกรรมหลัก จำนวน ๑๐ กิจกรรม ดังนี้

๓.๒.๑ การวิเคราะห์และออกแบบระบบ

๓.๒.๒ การจัดประชุมและสัมภาษณ์ผู้บริหาร

๓.๒.๓ การกำหนดโจทย์และข้อมูลที่เกี่ยวข้องกับโจทย์

๓.๒.๔ การกำหนดมาตรฐานข้อมูลและมาตรการในการปฏิบัติ

๓.๒.๕ การจัดหาฮาร์ดแวร์และซอฟต์แวร์

๓.๒.๖ การพัฒนาระบบบิ๊กดาต้าแพลตฟอร์ม

๓.๒.๗ การพัฒนาระบบบริหารจัดการข้อมูล

๓.๒.๘ การพัฒนาระบบวิเคราะห์ข้อมูลและทำรายงาน

๓.๒.๙ การทดสอบระบบที่พัฒนา

๓.๒.๑๐ การเชื่อมโยงข้อมูลด้านความมั่นคงทั้งภายในและภายนอกมาจัดเก็บที่คลังข้อมูล

๓.๒.๑๑ การวิเคราะห์ข้อมูลและทำรายงานแบบ Dashboard

๓.๒.๑๒ การฝึกอบรมบุคลากร

๓.๒.๑๓ การจัดทำเอกสารและคู่มือการใช้งานระบบ

๓.๒.๑๔ ส่งมอบระบบและรายงานปิดโครงการ

ตารางแสดงแผนการดำเนินงานในห้วงเวลา ๑๒ เดือน

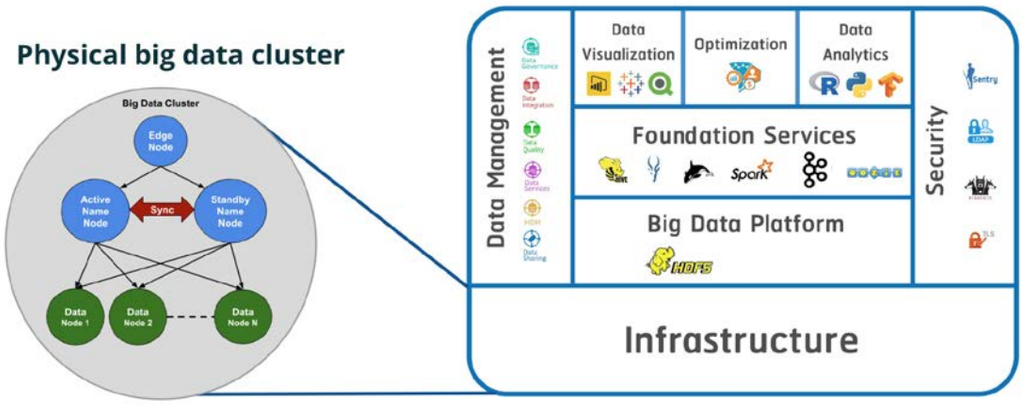
กิจกรรม	๑	๒	๓	๔	๕	๖	๗	๘	๙	๑๐	๑๑	๑๒
๑. วิเคราะห์และออกแบบระบบ												
๒. จัดประชุมและสัมภาษณ์												
๓. กำหนดโจทย์และข้อมูลที่เกี่ยวข้อง												

๔. กำหนดมาตรฐานและการปฏิบัติ												
๕. จัดหาฮาร์ดแวร์และซอฟต์แวร์												
๖. พัฒนาระบบบิ๊กดาต้าแพลตฟอร์ม												
๗. พัฒนาระบบบริหารจัดการข้อมูล												
๘. พัฒนาระบบวิเคราะห์ข้อมูล												
๙. ทดสอบระบบที่พัฒนา												
๑๐. เชื่อมโยงข้อมูลและทำคลังข้อมูล												
๑๑. วิเคราะห์ข้อมูลและทำรายงาน												
๑๒. ฝึกอบรมบุคลากร												
๑๓. จัดทำเอกสารและคู่มือการใช้งาน												
๑๔. ส่งมอบระบบและปิดโครงการ												

๓.๓ รายละเอียดการพัฒนาระบบตามแผนการดำเนินการในระยะที่ ๑ ปีที่ ๑

๓.๓.๑ ระบบบิ๊กดาต้าแพลตฟอร์ม (Big Data Platform)

ระบบบิ๊กดาต้านั้นพัฒนามาจากระบบแบบกระจาย (Distributed system) ซึ่งระบบที่นิยมใช้กันส่วนใหญ่จะพัฒนามาจาก Apache Hadoop ซึ่งเป็นซอฟต์แวร์ไม่มีลิขสิทธิ์หรือ Open source ดังนั้นการติดตั้งซอฟต์แวร์บริหารจัดการแพลตฟอร์ม จึงต้องการเครื่องแม่ข่ายหลายเครื่องมาทำงานร่วมกันเป็นกลุ่ม เรียกว่า คลัสเตอร์ (Cluster) โดยในคลัสเตอร์จะแบ่งเครื่องแม่ข่ายออกเป็นสองประเภท ได้แก่ เครื่องแม่ข่ายหลัก (Master node) ที่เป็นส่วนบริการหลักของบิ๊กดาต้าทำงานอยู่ โดยเฉพาะส่วนของตัวบริหารจัดการทรัพยากร (Resource manager) และตัวบริการจัดการงาน (Job manager) ซึ่งทำหน้าที่แบ่งงานหรือข้อมูลขนาดใหญ่ไปประมวลผลบนเครื่องแม่ข่ายสำหรับจัดเก็บและประมวลผลข้อมูล (Data node) โดยข้อมูลและงานบน Data node จะใช้เทคนิคการประมวลผลแบบขนาน (Parallel computing) เพื่อให้ระบบสามารถรองรับการทำงานกับข้อมูลขนาดใหญ่ได้และทำให้การประมวลผลมีประสิทธิภาพสูงขึ้น



แผนภาพที่ ๗ บิ๊กดาต้าคลัสเตอร์และแพลตฟอร์ม

แผนภาพที่ ๗ ทางด้านซ้ายแสดงบิ๊กดาต้าคลัสเตอร์ ที่ประกอบด้วยเครื่องแม่ข่ายหลัก (Master node) จำนวน ๓ เครื่อง ได้แก่ Active name node จำนวน ๑ เครื่อง Secondary name node จำนวน ๑ เครื่อง และ Edge node จำนวน ๑ เครื่อง และเครื่องแม่ข่ายจัดเก็บและประมวลผลข้อมูล (Data node) จำนวน ๓ เครื่อง เนื่องจากข้อมูลที่จัดเก็บในระบบไฟล์ของ Hadoop หรือ Hadoop file system (HDFS) จะถูกทำซ้ำสามชุดและแยกกันเก็บบน Data node ทั้งสามเครื่อง แสดงในแผนภาพที่ ๗ ด้านซ้าย ส่วนแผนภาพด้านขวาแสดงบิ๊กดาต้าแพลตฟอร์มที่พัฒนาบนระบบโครงสร้างพื้นฐาน (Infrastructure) ที่เป็นส่วนของ Master node และ Data node โดยแพลตฟอร์มที่พัฒนาขึ้นจะมีบริการพื้นฐาน (Foundation services) มาให้เพื่อรองรับงานที่หลากหลายและขนาดใหญ่ได้ ส่วนด้านบนสุดจะเป็นบริการในระดับสูง เช่น การวิเคราะห์ข้อมูล(Data analytics) การทำรายงานแบบแผนภาพ (Data visualization) และการให้บริการข้อมูล (Data service) เป็นต้น ส่วนสำคัญอีกสองส่วนได้แก่ ระบบบริหารจัดการข้อมูล (Data management) ด้านซ้ายของบิ๊กดาต้าแพลตฟอร์ม และระบบรักษาความปลอดภัย (Data security) ที่อยู่ด้านขวาของบิ๊กดาต้าแพลตฟอร์ม

แผนภาพที่ ๘ บริการพื้นฐานในบิ๊กดาต้าแพลตฟอร์ม

แผนภาพที่ ๘ แสดงบริการพื้นฐาน (Foundation services) ของ Hadoop ซึ่งแบ่งออกเป็นกลุ่มต่างๆ ได้แก่ ๑) บริการจัดเก็บและประมวลผล เช่น HDFS เป็นระบบไฟล์แบบกระจายของ Hadoop, Hive เป็นระบบฐานข้อมูลที่ทำงานบน HDFS และสนับสนุน SQL และ Spark เป็นระบบประมวลผลข้อมูลบนหน่วยความจำ (in-memory processing) ซึ่งมีประสิทธิภาพสูง ๒) บริการนำเข้าข้อมูล (Data ingestion) เช่น Sqoop สำหรับการนำเข้าข้อมูลแบบมีโครงสร้าง และ Flume สำหรับการนำเข้าข้อมูลแบบไม่มีโครงสร้าง ๓) บริการสายงานและการจัดตาราง (Workflow and scheduling) ที่ใช้บริการของ Oozie เป็นต้น ซึ่งบริการเหล่านี้จะถูกติดตั้งพร้อมกับระบบ Hadoop และถูกเรียกใช้โดยผู้ใช้หรือบริการในระดับบนต่อไป

เนื่องจากโครงการนี้เป็นระยะแรก จะยังไม่มี DR-site ที่เป็นบิ๊กดาต้าแพลตฟอร์มสำรอง แต่จะใช้การสำรองข้อมูลและการกู้คืนข้อมูล (Backup and Recovery) ตามมาตรฐานเช่นเดียวกัน โดยใช้การสำรองข้อมูล ทั้งหมดไปจัดเก็บไว้ใน Network storage ที่มีการเข้ารหัสไว้ และสามารถนำข้อมูลที่สำรองกลับคืนมาใช้งานได้ในกรณีที่ข้อมูลในระบบหลักชำรุดหรือสูญหายได้อย่างมีประสิทธิภาพ

๓.๓.๒ ระบบรักษาความปลอดภัยข้อมูล (Big Data Security)

ระบบรักษาความปลอดภัยข้อมูล แบ่งออกเป็น ๓ ด้าน ได้แก่ ความต้องการในการรักษาความปลอดภัย ระดับของความปลอดภัย และมาตรการด้านความปลอดภัย

๓.๓.๒.๑ ความต้องการในการรักษาความปลอดภัย (Security Requirements) แบ่งออกเป็น ๔ ด้านดังนี้

๓.๓.๒.๑.๑ Perimeter เป็นการป้องกันการภัยต่อความปลอดภัยของระบบประเภทต่างๆ ทั้งจากภายในและภายนอกระบบเครือข่าย ดังนั้นกลไกหรือเทคนิคในการแยกระบบเครือข่าย (network isolation) จึงถูกนำมาใช้ เช่น Firewall, router, subnet, public IP, private IP และ VPN เป็นต้น นอกจากการแยกส่วนของระบบเครือข่ายแล้ว การยืนยันบุคคล (Authentication) ก็เป็นสิ่งจำเป็นในการตรวจสอบว่าผู้ที่จะเข้าใช้งานระบบนั้นเป็นบุคคลที่อ้างถึงจริง

๓.๓.๒.๑.๒ Data ส่วนของข้อมูลภายในคลัสเตอร์นั้น ต้องได้รับการป้องกันจากการถูกเปิดเผยโดยผู้ไม่มีสิทธิ เช่นเดียวกับข้อมูลที่รับส่งระหว่างเครื่องหรือโหนดในระบบก็ต้องมีการป้องกันการถูกเปิดเผย ดังนั้นเทคนิค การเข้ารหัสข้อมูล (Data encryption) จึงถูกนำมาใช้ ทั้งข้อมูลที่จัดเก็บบนดิสก์ (Data encryption at rest) และข้อมูลที่รับส่งระหว่างโหนด (Data encryption in transit)

๓.๓.๒.๑.๓ Access การเข้าถึงบริการและข้อมูลต่างๆ ภายในระบบ จะต้องถูกยืนยันสิทธิก่อน การอนุญาตให้เข้าถึงได้ โดยใช้กลไกของการกำหนดสิทธิ (Authorization) เพื่อให้ผู้ที่ผ่านการยืนยันบุคคลแล้ว ได้รับสิทธิในการเข้าถึงบริการและข้อมูลตามที่ได้กำหนดเท่านั้น

๓.๓.๒.๑.๔ Visibility หมายถึงการที่ประวัติของข้อมูลได้ถูกตรวจสอบและติดตามไว้โดยที่ผู้ใช้ไม่ได้รับรู้ ผ่านทางกลไกของบริการตรวจสอบ (Auditing service) เพื่อรองรับการทำธรรมาภิบาลข้อมูล (Data governance) ซึ่งเป็นการตรวจสอบการเข้าถึงและใช้งานข้อมูลของผู้ใช้ในองค์กร ให้เป็นไปตามมาตรฐานที่ได้กำหนดไว้

๓.๓.๒.๒ ระดับของความปลอดภัย (Security Levels) ระดับของความปลอดภัยในการพัฒนาระบบบิ๊กดาต้า แบ่งออกเป็น ๔ ระดับ ดังนี้

๓.๓.๒.๒.๑ ระดับเริ่มต้น (Level 0) เป็นระดับที่ยังไม่มีการนำระบบรักษาความปลอดภัยมาใช้ เพื่อให้ผู้พัฒนาระบบได้ทำการทดสอบบริการต่างๆ ที่ติดตั้งในระบบว่าสามารถทำงานได้ครบถ้วนตามที่ต้องการ ก่อนที่จะมีระบบรักษาความปลอดภัยมาควบคุม หลังจากผู้พัฒนาระบบได้ทดสอบระบบจนมั่นใจว่าบริการต่างๆ ที่ติดตั้ง ที่ทำงานร่วมกันเป็นไปตามที่ต้องการแล้ว ผู้พัฒนาระบบจะเริ่มนำระบบรักษาความปลอดภัยเข้ามาบังคับใช้ ซึ่งถือว่าเป็นระดับที่ ๑

๓.๓.๒.๒.๒ ระดับที่ ๑ (Level 1) เป็นการนำกลไกรักษาความปลอดภัยมาใช้ในระดับต่ำสุด ซึ่งประกอบด้วย การยืนยันบุคคล (Authorization) โดยใช้ account แบบ local และการกำหนดสิทธิ (authorization) แบบ local เช่นเดียวกัน นอกจากนี้ยังมีระบบการตรวจสอบและติดตามการใช้งาน (Auditing) เพื่อให้ทราบว่าใครเข้ามาใช้ข้อมูลอะไร เมื่อไหร่ และใช้อย่างไร

๓.๓.๒.๒.๓ ระดับที่ ๒ (Level 2) เป็นการเพิ่มระดับความปลอดภัยจากระดับที่ ๑ โดยนำการเข้ารหัสข้อมูลมาใช้ (Data encryption) มีการบริหารจัดการรหัสลับ (Key management) รวมทั้งการตราวจสอบการใช้งานข้อมูลเชิงลึก สำหรับการทำธรรมาภิบาลข้อมูล (Data governance) ด้วย

๓.๓.๒.๒.๔ ระดับที่ ๓ (Level 3) เป็นระดับความปลอดภัยขั้นสูงสุด หรือเป็นความปลอดภัยระดับองค์กร (Enterprise Security) ซึ่งมีการเข้ารหัสข้อมูลทั้งส่วนที่จัดเก็บ (Data encryption at rest) และข้อมูลที่รับส่งผ่านระบบเครือข่าย (Data encryption in transit) กลไกการตรวจสอบและการทำธรรมาภิบาลข้อมูลเป็นไปตามมาตรฐานสากล เช่น NIST ซึ่งเป็นองค์กรกำกับมาตรฐานด้านต่างๆ รวมทั้งมาตรฐานด้านความปลอดภัย ในประเทศสหรัฐอเมริกา, HIPAA สำหรับระบบความปลอดภัยข้อมูลทางการแพทย์ และ PCI สำหรับระบบความปลอดภัยข้อมูลจากบัตรเครดิต เป็นต้น ที่สำคัญต้องมีการกำหนดขั้นตอนในการรักษาความปลอดภัย (Security procedure) ไว้อย่างละเอียดและเป็นมาตรฐานด้วย

๓.๓.๒.๓ มาตรการด้านความปลอดภัย (Security Procedure) เป็นการกำหนดแนวทางและกลไกในการปฏิบัติตนของผู้ใช้และเจ้าหน้าที่ ให้สามารถบริหารจัดการกับความเสี่ยงหรือภัยต่อระบบในด้านต่างๆ ที่อาจเกิดขึ้นในอนาคต และสอดคล้องกับมาตรฐานความปลอดภัยระดับสากล ซึ่งมี ๗ ด้าน ดังนี้

๓.๓.๒.๓.๑ Acceptable Use Policy (AUP) เป็นการกำหนดข้อตกลง สำหรับผู้ใช้ในองค์กร ที่ต้องปฏิบัติร่วมกันในการเข้าถึงหรือใช้งานระบบ เช่น ระบบเครือข่าย ระบบฐานข้อมูล ระบบแสดงรายงาน และระบบบิ๊กดาต้า เป็นต้น โดยเฉพาะเจ้าหน้าที่หรือพนักงาน ที่เริ่มเข้ามาทำงานใหม่ทุกคน ต้องได้รับการทำความเข้าใจในข้อตกลง และลงนามในเอกสารการยอมรับข้อตกลงนี้ตั้งแต่แรก

๓.๓.๒.๓.๒ Access Control Policy (ACP) เป็นแนวทางในการปฏิบัติสำหรับผู้ใช้ในองค์กร ในการเข้าถึงและการใช้งาน ทรัพยากร บริการ และข้อมูลของระบบ เช่น การกำหนดสิทธิการเข้าถึงของผู้ใช้แต่ละคนหรือแต่ละกลุ่ม ว่าสามารถเข้าถึง ระบบฐานข้อมูลใด ตารางใด หรือรายงานใดที่องค์กรมีอยู่ได้บ้าง รวมทั้งกำหนดสิทธิในการเข้าถึงข้อมูลหรือรายงานว่าสามารถดูได้อย่างเดียว หรือสามารถแก้ไขข้อมูลอะไรได้บ้าง ทั้งนี้รวมถึงการตรวจสอบและติดตาม (auditing) การเข้าถึงและใช้งานข้อมูลของผู้ใช้ในองค์กรด้วย นอกจากนี้ยังควรกำหนดแนวทางในการดำเนินการเมื่อผู้ใช้ออกจาก ระบบ เช่น ลาออกจากองค์กรไปแล้ว เป็นต้น

๓.๓.๒.๓.๓ Change Management Policy เป็นการกำหนดนโยบายอย่างเป็นทางการให้ผู้ใช้ในองค์กรปฏิบัติไปในแนวทางเดียวกัน ในการแก้ไขหรือเปลี่ยนแปลง อุปกรณ์ IT การให้บริการการใช้ทรัพยากรและข้อมูลในระบบ เป้าหมายของการกำหนดนโยบายนี้ เพื่อให้ผู้ใช้ทุกคนในองค์กร ได้รับ

ทราบหรือตระหนักถึงการเปลี่ยนแปลงนโยบายต่างๆ ในองค์กรทั่วกัน และทุกคนยอมรับการเปลี่ยนแปลงหรือแก้ไขนโยบายเหล่านั้น เพื่อให้การปฏิบัติเป็นไปอย่างถูกต้องเหมือนกัน

๓.๓.๒.๓.๔ Information Security Policy เป็นนโยบายระดับสูง ที่ครอบคลุมการเข้าถึงและใช้งานข้อมูลและสารสนเทศขององค์กร เพื่อให้ผู้ใช้ที่ใช้งานข้อมูลและสารสนเทศสอดคล้องกับกฎหรือระเบียบที่องค์กรกำหนดไว้ เช่น การกำหนดนโยบายในการเข้าถึงหรือดำเนินการกับข้อมูลและสารสนเทศที่มีชั้นความลับ หรือข้อมูลในการระบุตัวตนต่างๆ (Sensitive data) ซึ่งครอบคลุมการให้บริการและแลกเปลี่ยนข้อมูล (Data service and sharing) ทั้งภายในและภายนอกองค์กร

๓.๓.๒.๓.๕ Communication Policy เป็นการกำหนดกรอบในการติดต่อสื่อสารระหว่างผู้ใช้ภายในองค์กรด้วยสื่ออิเล็กทรอนิกส์ต่างๆ เช่น email, messenger, blog, chat และ social network เป็นต้น ตั้งแต่การกำหนดเทคโนโลยี หรือแอปพลิเคชั่นในการติดต่อสื่อสาร ที่สามารถใช้ได้บนเครื่องคอมพิวเตอร์ smart phone หรือ tablet ขององค์กร รวมทั้งแนวทางในการใช้งานสื่อเหล่านี้ได้อย่างเหมาะสม เพื่อไม่ให้เกิดผลกระทบหรือความเสียหายต่อภาพลักษณ์ขององค์กรและตัวบุคคล ในอนาคต

๓.๓.๒.๓.๖ Incident Response (IR) Policy เป็นการกำหนดแนวทางในการจัดการ กับเหตุการณ์ต่างๆ ที่ก่อให้เกิดความเสียหายกับระบบ ทรัพยากร หรือข้อมูล ในองค์กร การกำหนดมาตรการในการลดผลกระทบที่เกิดจากความสูญเสียในเหตุการณ์ที่เกิดขึ้น รวมทั้งการกำหนดระยะเวลาในการกู้คืนระบบ (system recovery) ที่เกิดจากความเสียหายต่างๆ

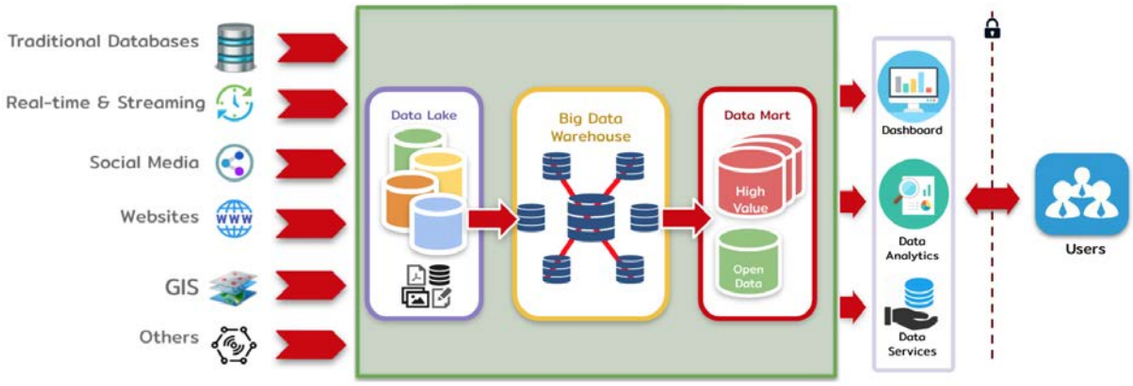
๓.๓.๒.๓.๗ Disaster Recovery Policy เป็นนโยบายที่ทำต่อเนื่องจาก IR Policy ซึ่งเป็นการกำหนดร่วมกันระหว่างบุคลากรด้าน cybersecurity และ IT เพื่อบริหารจัดการความสูญเสียจากเหตุการณ์ที่เกิดขึ้นมาแล้ว โดยเฉพาะการเน้นไปที่ระบบ ทรัพยากร และข้อมูลที่มีความสำคัญ จำเป็นต้องได้รับการสำรอง (Backup) และกู้คืน (Recovery) ได้ภายในระยะเวลาที่กำหนดไว้ใน IR Policy ทั้งนี้นโยบายในข้อ ๓.๓.๒.๓.๖ และ ๓.๓.๒.๓.๗ สามารถกำหนดร่วมกันได้ตามความเหมาะสม

๓.๓.๓ ระบบบริหารจัดการข้อมูล (Data Management System)

การบริหารจัดการข้อมูลในห้วงปีแรกจะมุ่งเน้น การวางพื้นฐานการบริหารจัดการในส่วนของ การนำเข้าข้อมูล (Data ingestion) และการบูรณาการข้อมูล (Data integration) ซึ่งเป็นการนำเข้าข้อมูลจากภายนอกมาจัดเก็บบน HDFS ในบิ๊กดาต้าแพลตฟอร์ม ซึ่งเป็นกระบวนขั้นพื้นฐานที่จำเป็นดังแสดงใน แผนภาพที่ ๙ กระบวนการในการบริหารจัดการข้อมูล (Data management process) โดยเริ่มจากการนำเข้าข้อมูลทั้งแบบมีโครงสร้าง (Structured data) เช่น ระบบฐานข้อมูลแบบสัมพันธ์ (RDBMS) และข้อมูลแบบไม่มีโครงสร้าง (Unstructured data) เช่น ข้อมูลจาก log file ของเครื่องแม่ข่าย หรือข้อมูลกึ่งโครงสร้าง (Semi-structured data) เช่น ไฟล์เอกสาร XML, Excel และ CSV เป็นต้น โดยข้อมูลเหล่านี้จะถูกนำเข้ามาจัดเก็บบน HDFS ในทะเลสาบข้อมูล (Data lake) ที่เป็นพื้นที่ส่วนแรกของบิ๊กดาต้าแพลตฟอร์ม ซึ่งก่อนการจัดเก็บจะต้องมีการตรวจสอบคุณภาพข้อมูล และการทำความสะอาดข้อมูล ด้วยบริการพื้นฐานหรือเครื่องมือบริหารจัดการข้อมูลโดยวิศวกรข้อมูล (Data engineer)

จากนั้นนักวิเคราะห์ข้อมูล (Data analyst) หรือนักวิทยาศาสตร์ข้อมูล (Data scientist) จะนำข้อมูลในทะเลสาบข้อมูล (Data lake) มาวิเคราะห์และเลือกเฉพาะข้อมูลที่เกี่ยวข้องกับโจทย์หรือการนำไปใช้ โดยผ่านกระบวนการ ETL ที่แปลงข้อมูลจากทะเลสาบข้อมูล (Data lake) ซึ่งมีรูปแบบไม่ต่างจากข้อมูลต้นทาง ให้อยู่ในรูปแบบข้อมูลที่นักวิเคราะห์ต้องการในคลังข้อมูล (Data warehouse) ซึ่งอาจจัดเก็บในรูปแบบของ

ข้อมูลแบบมีโครงสร้าง ที่สนับสนุน SQL หรือไม่ก็ได้ เช่น Hive จะสนับสนุนการใช้ภาษา SQL ในการ query ข้อมูล ส่วน HBase จะสนับสนุนการใช้ NoSQL ในการจัดการข้อมูลบนระบบบิ๊กดาต้าของ Hadoop เป็นต้น และสุดท้ายข้อมูลใน Data warhouse จะถูกนำไปวิเคราะห์ เพื่อคาดการณ์แนวโน้มสถานการณ์ รวมทั้งกำหนดหนทางปฏิบัติที่เหมาะสม (Optimization) ในการแก้ไขปัญหาภัยคุกคามด้านความมั่นคงที่เกิดขึ้น โดยจัดเก็บอยู่ในตลาดข้อมูล (Data mart) ก่อนจะถูกนำไปใช้ในการวิเคราะห์และทำรายงาน หรือการให้บริการข้อมูลกับผู้ใช้ในระดับต่างๆ ต่อไป



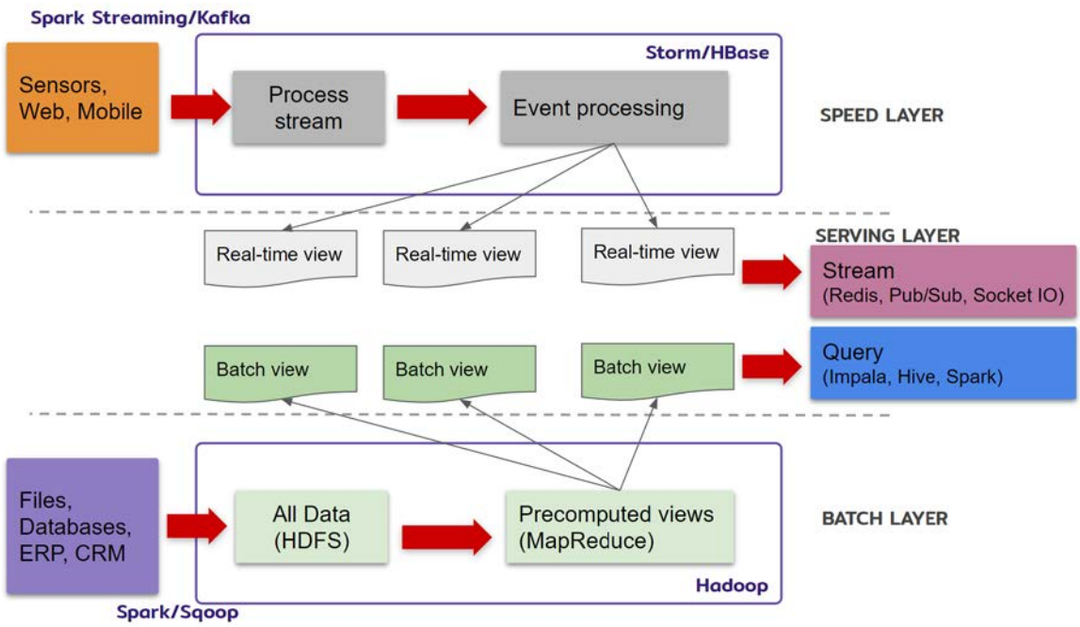
แผนภาพที่ ๙ กระบวนการบริหารจัดการข้อมูลขั้นพื้นฐาน

๓.๓.๓.๑ การนำเข้าข้อมูล (Data ingestion) และการบูรณาการข้อมูล (Data integration)

การนำเข้าข้อมูลและการบูรณาการข้อมูล เป็นกระบวนการพื้นฐานสำคัญของการทำ ETL (Extract, Transform Load) ที่จำเป็นจะต้องมีการนำข้อมูลจากแหล่งข้อมูลต่างๆ มาเก็บไว้ในทะเลสาบข้อมูล (Data lake) และปรับเปลี่ยนโครงสร้างรวมทั้งปรับปรุงคุณภาพ เพื่อจัดเก็บใน Data warehouse สำหรับให้นักวิทยาศาสตร์ข้อมูลได้เข้ามาใช้วิเคราะห์และใช้ประโยชน์ รวมถึงการให้บริการข้อมูลผ่านตลาดข้อมูล (Data mart) และ Open data ซึ่งแหล่งข้อมูลต่างๆ อาจจะประกอบไปด้วย Sensors ที่ผลิตข้อมูลแบบ Realtime และระบบฐานข้อมูลต่างๆ เช่น MySQL, Microsoft SQL Server หรือ ORACLE ของแต่ละหน่วยงาน ระบบเว็บไซต์ที่มีการจัดเก็บและเผยแพร่ข้อมูลข่าวสาร ระบบสื่อสังคมออนไลน์ที่เป็นแหล่งเก็บข้อมูลการพูดคุยแลกเปลี่ยนแสดงความรู้สึก รวมทั้งระบบ Enterprise Resource Planning (ERP) และ Customer Relationship Management (CRM) แหล่งข้อมูลเหล่านี้จะแยกอยู่ตามหน่วยงานต่างๆ โดยส่วนใหญ่หน่วยงานเจ้าของระบบจะเป็นผู้ดูแลและเป็นเจ้าของข้อมูล ซึ่งแหล่งข้อมูลเหล่านี้จะถูกจัดเก็บในลักษณะของ Silo ที่แต่ละ Silo จะมีรูปแบบและโครงสร้างของข้อมูลที่แตกต่างกัน และส่วนใหญ่ไม่ได้มีการเชื่อมโยงกัน

โครงสร้างสถาปัตยกรรมของข้อมูลแบบ Silo (Silo-based architecture) จะทำให้การวิเคราะห์ข้อมูลขนาดใหญ่ที่ต้องการผลในทันที (Real-tiem insights) เป็นไปไม่ได้ จำเป็นอย่างยิ่งที่ข้อมูลต่างๆจะต้องมีการจัดเก็บในทะเลสาบข้อมูล (Data lake) ในลักษณะรวมศูนย์และอยู่ในระบบบิ๊กดาต้าแพลตฟอร์มเดียวกันจึงจะทำให้การคำนวณและการวิเคราะห์ข้อมูลขนาดใหญ่ต่างๆเป็นไปได้ ซึ่งต้องอาศัยคอมพิวเตอร์ที่มีระบบการประมวลข้อมูลผลขนาดใหญ่ และทำให้การควบคุมดูแลข้อมูลแบบรวมศูนย์เป็นไปได้ง่ายด้วย การนำ เข้าข้อมูลสามารถทำได้หลายแบบ ทั้งแบบ Real-time และ Batch ซึ่งการนำเข้าแบบ Real-

time ข้อมูลต้นทางและข้อมูลปลายทางในทะเลสาบข้อมูล (Data lake) จะเหมือนกันเสมอ การนำเข้าข้อมูลจะเป็นลักษณะไหลเข้าตลอดเวลา ส่วนการนำเข้าแบบ Batch จะเป็นลักษณะเป็นการนำเข้าข้อมูลเป็นครั้งคราวตามตารางเวลาที่กำหนด เช่น การนำเข้าทุก ๑๕ นาที รายวัน หรือแม้แต่รายเดือน เป็นต้น ซึ่งวิธีการนำเข้าข้อมูลมีได้ หลายรูปแบบ แผนภาพที่ ๑๐ แสดงสถาปัตยกรรมการนำเข้าข้อมูลแบบ Lambda (Lambda Arcitecture) ซึ่งเป็นสถาปัตยกรรมที่เป็นที่นิยมที่สามารถนำเข้าข้อมูลทั้งแบบ Real-time streaming และ Batch ได้ในคราวเดียว โดยใช้เทคโนโลยีและกระบวนการที่แตกต่างกัน ในภาพแสดงตัวอย่างเทคโนโลยีที่ใช้เช่น ใช้ Spark Streaming และ Kafka ในการนำเข้าข้อมูลแบบ Real-time และใช้ Spark และ Sqoop ในการนำเข้าข้อมูลแบบ Batch เป็นต้น



แผนภาพที่ ๑๐ ตัวอย่างสถาปัตยกรรมของการนำเข้าข้อมูลแบบ Lambda

๓.๓.๓.๒ การตรวจสอบคุณภาพข้อมูล (Data quality)

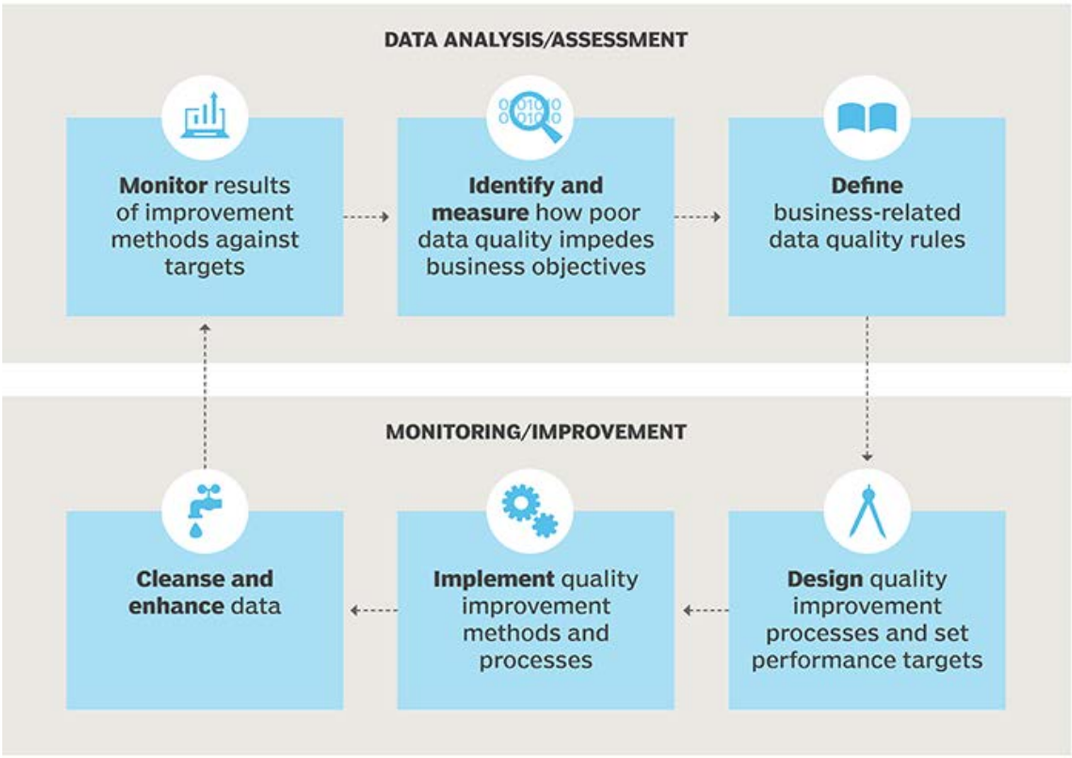
จากคำกล่าวเปรียบเปรยที่ว่า “Garbage in garbage out” หมายถึง การใช้ข้อมูลที่ไม่ถูกต้องและไม่มีคุณภาพไปทำการวิเคราะห์ ก็จะส่งผลให้ผลลัพธ์จากการวิเคราะห์ไม่ถูกต้อง ดังนั้นการตรวจสอบคุณภาพข้อมูล (Data quality) จึงเป็นขั้นตอนที่สำคัญ ในการปรับปรุงให้ข้อมูลมีความถูกต้องและมีคุณภาพ ซึ่งเมื่อนำไปใช้ในการวิเคราะห์ จะส่งผลให้ผลการวิเคราะห์มีความถูกต้องและมีคุณภาพเช่นกัน ขั้นตอนนี้จะช่วยกลั่นกรองข้อมูลที่นำเข้าจากต้นทางว่ามีคุณภาพเป็นอย่างไร เนื่องจากข้อมูลต้นทางที่ใช้การจัดเก็บด้วยระบบแบบดั้งเดิม (Traditional data entry) ที่ใช้เจ้าหน้าที่บันทึกข้อมูล ซึ่งอาจมีความผิดพลาดหรือความซ้ำซ้อนของข้อมูลเกิดขึ้นได้ โดยทั่วไปการตรวจสอบคุณภาพข้อมูลสามารถทำได้หลายวิธี เช่นการตรวจสอบโดยสายตาซึ่งต้องอาศัยเวลา หรือการตรวจสอบโดยใช้เครื่องมือวิเคราะห์ต่างๆ หรือการใช้คนร่วมกับเครื่องมือ โดยทั่วไปมิติที่ใช้ในการวัดคุณภาพข้อมูล ดังแสดงในแผนภาพที่ ๑๑ ประกอบไปด้วย ความถูกต้องของข้อมูล (Accuracy) ความสมบูรณ์ของข้อมูล (Completeness) ความคงเส้นคงวาของข้อมูล

(Consistency) หรือไม่ขัดแย้งกันเอง มีความชัดเจน (Clarity) มีโครงสร้างที่ดี (Structure) และมีความทันสมัย (Timliness) เป็นต้น ซึ่งกระบวนการปรับปรุงคุณภาพข้อมูลจะต้องใช้เวลา อาศัยผู้รู้และคุ้นเคยกับข้อมูล รวมถึงมีอุปกรณ์ต่างๆ ในการช่วยให้การตรวจสอบคุณภาพข้อมูลได้ผลที่แม่นยำและรวดเร็ว

แผนภาพที่ ๑๑ ตัวอย่างมิติแสดงคุณภาพของข้อมูล

๓.๓.๓.๓ การทำความสะอาดข้อมูล (Data cleansing)

การทำความสะอาดข้อมูล (Data cleansing) เป็นขั้นตอนหนึ่งในวงจรของการบริหารจัดการคุณภาพข้อมูล (Data quality management cycle) ดังที่แสดงในแผนภาพที่ ๑๒ เพื่อลบความซ้ำซ้อนของข้อมูล และการปรับแก้ข้อมูลที่คลาดเคลื่อน โดยในวงจรจะแบ่งออกเป็น ๒ ขั้นตอนใหญ่ๆ คือ ขั้นตอนการวิเคราะห์และตรวจสอบคุณภาพ (Data Analysis/Assessment) ซึ่งประกอบไปด้วยขั้นตอนการเฝ้าระวัง (Monitor) ขั้นตอนการค้นหาและวัดข้อบกพร่องของข้อมูล (Identify and measure) และขั้นตอนการกำหนดกฎเกณฑ์ต่างๆ ในการควบคุมคุณภาพข้อมูล (Define quality rules) ส่วนขั้นตอนที่ ๒ คือการเฝ้าระวังและปรับปรุงข้อมูล (Monitoring/Improvement) ซึ่งประกอบไปด้วย ขั้นตอนการออกแบบและการกำหนดเป้าหมาย (Design data quality improvement process) ขั้นตอนการกำหนดระบบปรับปรุงข้อมูล (Data Quality Process Impremention) และสุดท้ายขั้นตอนการดำเนินการทำความสะอาดและปรับปรุงข้อมูล (Data Cleansing and Enhancement) ซึ่งเป็นกระบวนการวนกลับที่เป็นวงจรอย่างไม่สิ้นสุด ในปัจจุบันเครื่องมือที่สามารถช่วยให้การทำงานทำได้ง่าย สะดวก รวดเร็ว และมีความถูกต้องมากขึ้น เช่น เครื่องมือการเตรียมข้อมูล (Data preparation) และเครื่องมือ Data Stewadship ที่ช่วยให้เจ้าของข้อมูลสามารถทำการปรับปรุงข้อมูลที่ตนเองรับผิดชอบได้ง่ายและมีมาตรฐาน



แผนภาพที่ ๑๒ วงจรการบริหารจัดการคุณภาพข้อมูล (Data qulaity management cycle)
ที่มา: TechTarget.com

๓.๓.๓.๔ การบริการข้อมูล (Data services)

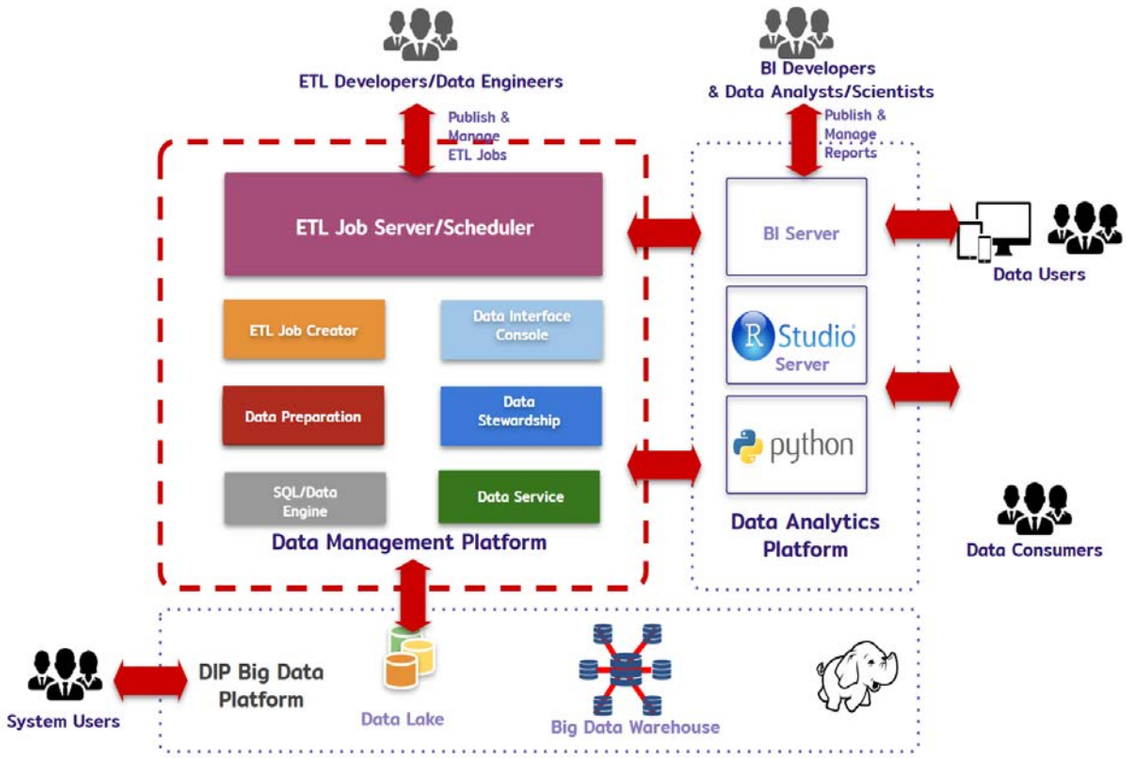
การให้บริการข้อมูล (Data Services) ถือเป็นส่วนหนึ่งของงานการบริหารและจัดการข้อมูล เพื่อสนับสนุนการสร้างระบบ ในการให้บริการด้านข้อมูลและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน และแอปพลิเคชัน ไม่ว่าจะเป็นในรูปแบบของ REST web services หรือ Enterprise service bus (ESB) เพื่อให้การรวบรวมและแลกเปลี่ยนข้อมูลในรูปแบบต่างๆ จากหลายๆ แหล่ง สามารถทำได้ง่ายและสะดวกขึ้น มีความปลอดภัยและมีระบบจัดการที่มีประสิทธิภาพ เป็นการทำให้หน่วยงานและผู้บริโภคข้อมูลต่างๆ สามารถเข้าถึงข้อมูลได้ง่ายขึ้น ทำให้เกิดการใช้ประโยชน์ข้อมูลได้อย่างกว้างขวางมากขึ้น

๓.๓.๓.๕ ส่วนประกอบของระบบ Data Management

สรุปส่วนประกอบของระบบการบริหารจัดการข้อมูลควรจะประกอบไปด้วยส่วนประกอบหลักๆดังที่แสดงในแผนภาพที่ ๑๓ ดังนี้

๓.๓.๓.๕.๑ ส่วน ETL Job Server and Scheduler สำหรับจัดเก็บ บริหาร ตรวจสอบสถานะ จัดตารางการรันและประมวลผลโปรแกรมงานด้าน ETL ต่างๆ

๓.๓.๓.๕.๒ ส่วน ETL Job Creator สำหรับเป็นเครื่องมือในการสร้างโปรแกรมงานด้าน ETL ที่ต้องง่ายต่อการใช้งานและควรจะเป็นลักษณะ Drag-and-drop UI เพื่อให้การเขียนโปรแกรมสามารถทำได้ง่ายโดยไม่ต้องเขียนโค๊ด



แผนภาพที่ ๑๓ ส่วนประกอบหลักของระบบ Data Managment

๓.๓.๓.๕.๓ ส่วน Data Interface Console สำหรับเป็นช่องทางการเข้าถึงข้อมูลที่อยู่ในระบบบิ๊กดาต้าแพลตฟอร์ม เพื่อให้ผู้ใช้สามารถเข้าถึงแหล่งข้อมูล และบริหารจัดการข้อมูลได้ง่าย ผ่านเว็บไซต์

๓.๓.๓.๕.๔ ส่วนเครื่องมือ Data preparation เพื่อเป็นเครื่องมือในการเตรียมข้อมูลและตรวจวิเคราะห์คุณภาพข้อมูล

๓.๓.๓.๕.๕ ส่วนเครื่องมือ Data stewardship สำหรับเป็นช่องทางให้เจ้าหน้าที่บริการข้อมูล (Data steward) ได้สามารถเข้าถึงข้อมูลเพื่อตรวจสอบและปรับปรุงข้อมูลได้เอง โดยไม่ต้องพึ่งเจ้าหน้าที่ IT เป็นผู้ปรับปรุงข้อมูล

๓.๓.๓.๕.๖ ส่วน SQL/Data Engine สำหรับให้เจ้าหน้าที่ Data Engineers สามารถเขียนโปรแกรมเพื่อประมวลผลข้อมูลโดยใช้ภาษาที่คุ้นเคย เช่น ภาษา SQL เพื่อใช้ในการประมวลผลข้อมูลขนาดใหญ่

๓.๓.๓.๕.๗ ส่วน Data service ทำหน้าที่ในการบริหารจัดการ และอำนวยความสะดวกงานด้านการบริการ เชื่อมโยงและแลกเปลี่ยนข้อมูลกับผู้ใช้ข้อมูล หน่วยงานอื่นๆ และระบบต่างๆจากภายนอก

๓.๓.๔ ระบบวิเคราะห์ข้อมูลและทำรายงาน (Data Analytics and Visualization)

การวิเคราะห์ข้อมูล (Data analytics) เป็นศาสตร์ที่ถูกนำมาใช้ในงานบิ๊กดาต้า ที่ใช้การวิเคราะห์ด้วยสถิติหรือฟังก์ชันทางคณิตศาสตร์ กับข้อมูลที่มีแนวโน้มว่าจะมีขนาดใหญ่หรือมีความหลากหลายรอบด้านมากขึ้นกว่าแต่ก่อน ทำให้ได้ผลการวิเคราะห์เชิงลึกมากขึ้น โดยผลลัพธ์ที่ได้นี้จะยังอยู่ในรูปแบบของตัวเลขหรือข้อความเป็นส่วนใหญ่ จึงต้องมีการทำรายงานแบบแผนภาพ (Data visualization) ซึ่งเป็นการนำเสนอ

ผลการวิเคราะห์ข้อมูลในรูปแบบของกราฟต่างๆ และสามารถนำมารวมกันเป็น Dashboard ที่มีส่วนติดต่อผู้ใช้แบบโต้ตอบ (Interactive interface) ทำให้ผู้ใช้สามารถปรับเปลี่ยนมุมมองของกราฟตามตัวเลือกที่ผู้ใช้กำหนดบน Dashboard ได้ สำหรับการวิเคราะห์และทำรายงานของบิ๊กดาต้าสามารถแบ่งออกได้เป็นหลายประเภท ดังนี้

๓.๓.๔.๑ Descriptive analytics เป็นการวิเคราะห์ข้อมูลเชิงพรรณนาโดยมีจุดประสงค์หลักเพื่อรู้ถึงสถานการณ์หรือสถานภาพปัจจุบัน เพื่อตอบคำถามหลักว่า “เกิดอะไรขึ้น” โดยผลลัพธ์ของการดำเนินการวิเคราะห์ในขั้นนี้จะเป็นผลสรุปเชิงสถิติต่างๆ ในลักษณะdashboardหรือรายงานสรุปสถานภาพรวมไม่ว่าจะเป็นรายงานประจำขั้นพื้นฐาน (Canned Reporting) หรือเป็นรายงานเฉพาะกิจ (Ad Hoc Reporting)

๓.๓.๔.๒ Diagnostic analytics เป็นการวิเคราะห์ข้อมูลเชิงหาสาเหตุโดยมีจุดประสงค์หลักเพื่อหาสาเหตุหรือปัจจัยที่มีผลเกี่ยวเนื่องกับการเกิดขึ้นของเหตุการณ์ใดเหตุการณ์หนึ่ง หรือโดยส่วนใหญ่จะมุ่งไปที่สาเหตุของปัญหา เพื่อตอบคำถามหลักที่ว่า “ทำไมถึงเกิดขึ้น” โดยขั้นตอนนี้จะเป็นการวิเคราะห์โดยอาศัย dashboard หรือรายงานและความสามารถในการกรองข้อมูล (Filter) และการเจาะลึกศึกษาข้อมูลจากกลุ่มใหญ่ไปยังกลุ่มย่อย เพื่อให้ได้มาซึ่งข้อมูลเชิงลึก (Insign) บอกถึงความเชื่อมโยงหรือสาเหตุของสิ่งที่เกิดขึ้น

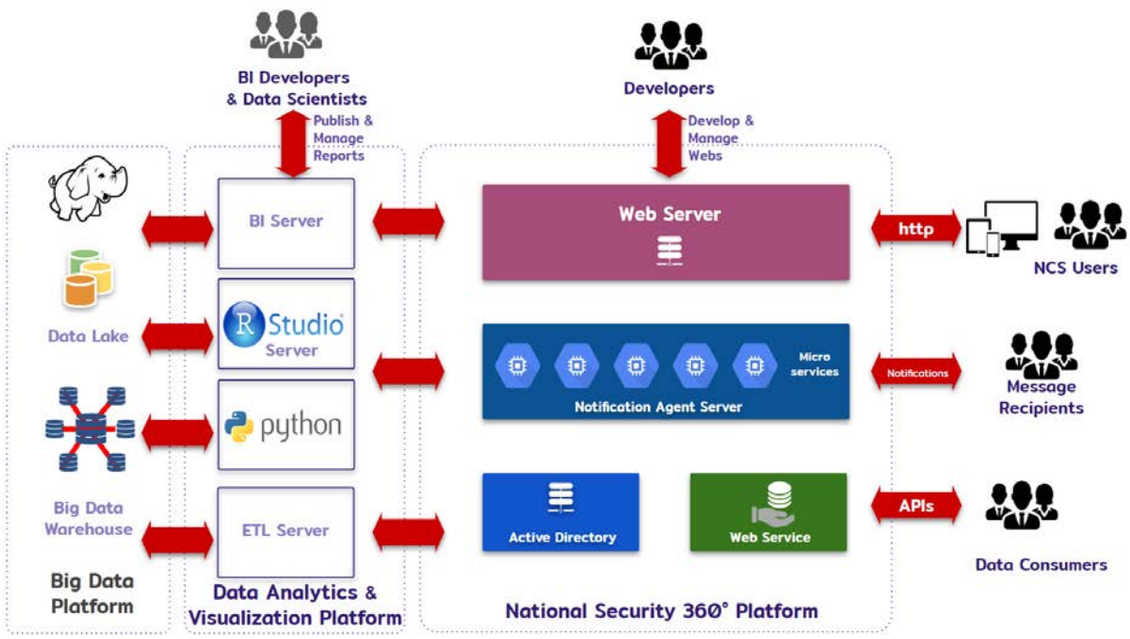
๓.๓.๔.๓ Predictive analytics เป็นการวิเคราะห์ข้อมูลเชิงพยากรณ์โดยมีจุดประสงค์หลักเพื่อ หาความสัมพันธ์ของเหตุและผลที่เกิดขึ้นของเหตุการณ์หรือปัญหา เพื่อตอบคำถามหลักที่ว่า “เกิดขึ้นได้อย่างไร” โดยขั้นตอนนี้เป็นการวิเคราะห์สร้างโมเดล (Model) ที่แสดงถึงแบบแผนการเกิด (Pattern) หรือความสัมพันธ์ของปัจจัยที่เป็นสาเหตุทั้งหมด (features หรือ predictors) กับผลลัพธ์ที่เกิด (response) โดยอาศัยกระบวนการ Machine Learning ในการสร้างโมเดลเพื่อที่จะใช้พยากรณ์แนวโน้มหรือผลลัพธ์ที่จะเกิดขึ้นในอนาคตจากข้อมูลปัจจุบันซึ่งเป็นการตอบคำถาม “จะเกิดอะไรขึ้นต่อไป” ซึ่งโมเดลที่ได้ในขั้นนี้แยกเป็น ๒ ประเภทคือ Regression Model ใช้ในการพยากรณ์ข้อมูลเชิงปริมาณ และ Classification Model ใช้ในการพยากรณ์ข้อมูลเชิงคุณภาพ

๓.๓.๔.๔ Prescriptive analytics เป็นการวิเคราะห์เชิงเยียวยาหรือเชิงบรรเทา โดยมีจุดประสงค์หลักเพื่อกำหนดการดำเนินการขั้นถัดไปให้ได้ผลลัพธ์ที่ดีมีประสิทธิภาพมากที่สุด (Optimization) โดยจะเป็นการตอบคำถามหลักที่ว่า “การดำเนินการที่ดีที่สุดคืออะไร” โดยขั้นตอนนี้จะเป็นการบูรณาการการวิเคราะห์ข้อมูลในทุกขั้นตอนเข้าด้วยกันเพื่อสร้างเป็นระบบที่ช่วยในการตัดสินใจเพื่อดำเนินการในสิ่งที่คาดการณ์ว่าจะส่งผลลัพธ์ที่ดีที่สุด

๓.๓.๕ ระบบวิเคราะห์และแจ้งเตือนเพื่อความมั่นคงแห่งชาติ ๓๖๐° (National Security Analytics and Notifications 360°)

ระบบวิเคราะห์และแจ้งเตือนเพื่อความมั่นคงแห่งชาติ ๓๖๐° เป็น เครื่องมือที่ใช้ในการวิเคราะห์ และแสดงผลการวิเคราะห์ข้อมูลด้านความมั่นคงรอบด้าน แทนการพัฒนาจากซอฟต์แวร์ประเภทธุรกิจอัจริยะ หรือ Business Intelligence (BI) ในการทำการออกแบบและสร้าง Dashboard แบบ Interactive ต่างๆ ชุดอุปกรณ์เหล่านี้ ออกแบบมาเพื่อให้ผู้บริหารและเจ้าหน้าที่ที่เกี่ยวข้อง สามารถเข้าใช้และเข้าถึงข้อมูลได้ง่าย ช่วยให้สามารถวิเคราะห์และตัดสินใจได้อย่างแม่นยำ และช่วยเปลี่ยนสภาพข้อมูล (Data) ไปสู่ข้อมูลเชิงลึก (Insights) และองค์ความรู้ (Knowledge) สุดท้ายทำให้ผู้ใช้สามารถติดสินใจได้อย่างชาญฉลาด (Make smart decision) แล้วนำไปปฏิบัติจนเกิดผล (Take smart action) เพื่อช่วยเพิ่มขีดความสามารถการ

ปฏิบัติงาน ด้านความมั่นคงได้อย่างชาญฉลาดและสะดวก แต่มีข้อจำกัดคือจำเป็นต้องติดตั้ง หรือมีชุดอุปกรณ์เหล่านี้ทุก ครั้ง เมื่อต้องการใช้หรือนำเสนอและแสดงผลรายงานจะไม่สามารถรองรับผู้ใช้จำนวนมากได้ และอาจจะไม่สามารถตอบสนอง ต่อความต้องการของระบบของสำนักงานสภาความมั่นคงแห่งชาติได้ทั้งหมด โดยเฉพาะ ความต้องการระบบการแจ้งเตือนแบบ Real-Time ที่จำเป็นจะต้องมีการแจ้งเตือนผลจากการวิเคราะห์ทุกครั้งให้ผู้ที่เกี่ยวข้องรับทราบทันที เพื่อให้ผู้เกี่ยวข้องสามารถดำเนินงานตามภารกิจความรับผิดชอบได้อย่างรวดเร็วและทันท่วงที ผู้ใช้ทุกระดับชั้นต้องสามารถเข้าใช้และเข้าถึง Dashboard ต่างๆ ได้ง่าย ทุกที่ทุกเวลา และสามารถรับข้อมูลการแจ้งเตือนได้ทุกที่ทุกเวลาเช่นกัน โดยสามารถเข้าถึงและใช้ระบบผ่านหน้าเว็บไซต์และชุดอุปกรณ์มือถือแบบ Smartphone ซึ่งมีสถาปัตยกรรมระบบดังแสดงในแผนภาพที่ ๑๔



แผนภาพที่ ๑๔ สถาปัตยกรรมระบบแสดงผลการวิเคราะห์และแจ้งเตือนเพื่อความมั่นคงแห่งชาติ ๓๖๐°

แผนภาพที่ ๑๔ แสดงตัวอย่างส่วนประกอบหลักและระบบที่เกี่ยวข้องกับระบบ National Security Analytics and Notifications 360° หรือสามารถเรียกสั้นๆ ว่าระบบ National Security 360° ซึ่งเป็น User Interface (UI) หลักในการให้ผู้ใช้เข้าถึงและเข้าใช้ระบบบิ๊กดาต้าแพลตฟอร์มและระบบวิเคราะห์ข้อมูลขนาดใหญ่ จากซ้ายของแผนภาพแสดงข้อมูลต่างๆ และการประมวลผลข้อมูลขนาดใหญ่ต่างๆ จะถูกจัดเก็บไว้และทำในระบบระบบบิ๊กดาต้าแพลตฟอร์มซึ่งถูกต่อเชื่อมกับระบบ Data Analytics and Visualization Platform ซึ่งมีการติดตั้ง Servers และชุดอุปกรณ์สำหรับการวิเคราะห์ข้อมูล เช่น ชุดระบบ BI Server สำหรับการพัฒนา จัดเก็บ และติดตั้งรายงานและ dashboard การวิเคราะห์ข้อมูลต่างๆ ชุดระบบ R Studio Server และ Python สำหรับเป็นเครื่องมือหลักของนักวิเคราะห์ข้อมูล (Data Analysts) และนักวิทยาศาสตร์ข้อมูล (Data Scientists) ในการทำการวิเคราะห์และทำ Machine Learning Models ต่างๆ และชุดระบบ ETL Server สำหรับเป็นชุดในการบริหารจัดการข้อมูล ในการนำเข้าข้อมูลจากหลายแหล่งข้อมูล (Data

Ingestion) และงานด้าน ETL (Extract-Transform-Load) และ ELT (Extract-Load-Transform) ในการทำความสะอาดข้อมูล (Data Cleansing) และปรับเปลี่ยนโครงสร้างและสภาพของข้อมูลให้ถูกต้อง มีระเบียบและตรงตามความต้องการของแต่ละการวิเคราะห์ข้อมูล เป็นต้น ในส่วนของระบบ National Security 360° ทางขวาสุดของแผนภาพ จะเป็นส่วนประกอบหลักสำหรับให้ผู้ใช้เข้าถึงและเข้าใช้ระบบ ซึ่งประกอบด้วย ๔ ระบบหลัก ดังนี้

๓.๓.๕.๑ ระบบ Web Server สำหรับติดตั้งเว็บ Application ซึ่งจะเป็นช่องทางหลักในการเข้าถึงข้อมูลการวิเคราะห์และใช้รายงานและ dashboard ต่างๆ ของผู้ใช้ทุกระดับชั้นผ่านหน้าเว็บไซต์ รวมถึงการใช้เป็นที่ติดตั้งระบบบริหารจัดการรายงานและ Dashboard และระบบบริหารจัดการผู้ใช้ระดับต่างๆ ในการกำหนดสิทธิการเข้าถึงรายงานและชุดข้อมูล Mobile Application และช่องทางการเข้าถึงและใช้ Web Services และการแจ้งเตือนข้อความต่างๆด้วย

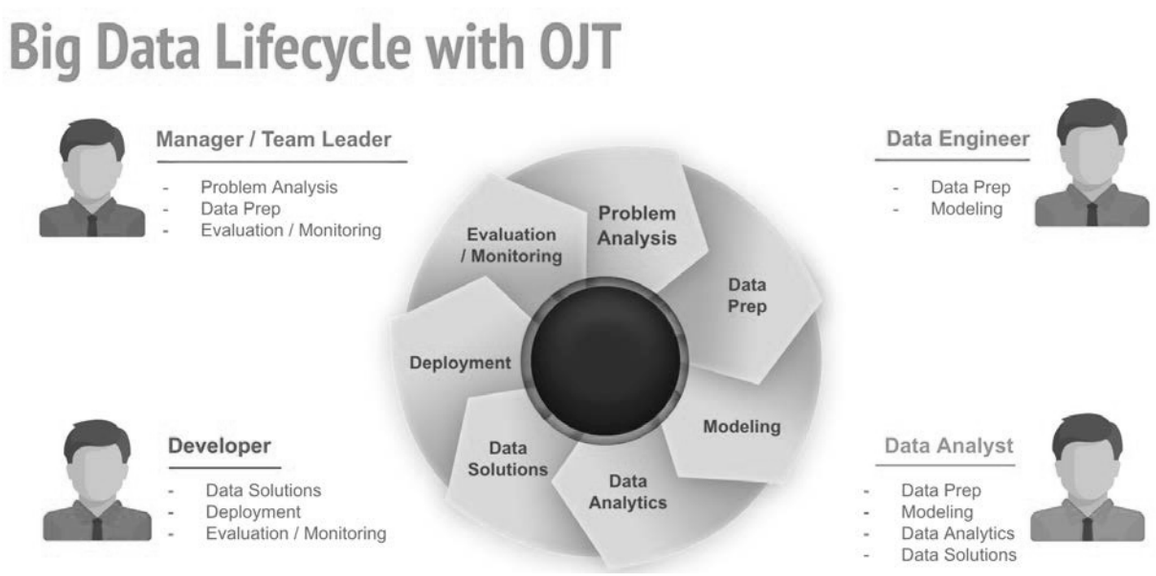
๓.๓.๕.๒ ระบบ Notification Agent Server สำหรับติดตั้งชุด Notification Microservice Agent ต่างๆ ในการทำหน้าที่บริหารจัดการและทำหน้าที่แจ้งเตือนแบบ Push Notification เพื่อส่งผลการวิเคราะห์ข้อมูลและข้อความต่างๆ ไปยังผู้ใช้กลุ่มต่างๆ ตามที่ออกแบบและกำหนดไว้อย่างถูกต้อง และ Real-time

๓.๓.๕.๓ ระบบ Active Directory เป็นเครื่องมือสำหรับทำหน้าที่ช่วยจัดการทรัพยากรในระบบ บริหารจัดการทรัพยากรผู้ใช้ระบบ (User) บริหารจัดการความปลอดภัยให้กับระบบโดยรวม และทำหน้าที่จัดเก็บข้อมูลเกี่ยวกับ Object ต่างๆ เช่น ผู้ใช้ระบบ (User) กลุ่มผู้ใช้ (User Group) คอมพิวเตอร์ (Computer) และ นโยบายรักษาความปลอดภัย (Security Policy) เป็นต้น ซึ่งหน้าที่หลักในระบบนี้คือ บริหารจัดการสิทธิ์การเข้าใช้ระบบของ ผู้ใช้ และกำหนดกลุ่มและสิทธิ์การเข้าถึงและใช้ข้อมูลรายงาน dashboard และการแจ้งเตือนต่างๆ ตามระดับชั้นความลับ หรือตามนโยบายรักษาความปลอดภัยข้อมูลต่างๆ และเป็นตัวหลักในการกำหนดสิทธิการเข้าถึง Web Application และ Mobile Application

๓.๓.๕.๔ ระบบ Web Service เป็นระบบสำหรับติดตั้งส่วนบริการข้อมูลต่างๆแบบ Web Services ประกอบด้วย Web APIs ต่างๆในการบริการข้อมูลให้กับหน่วยงานและผู้บริโภคข้อมูล ในการตอบสนองต่อนโยบายการเชื่อมต่อ และแลกเปลี่ยนข้อมูลที่มีประโยชน์ระหว่างหน่วยงาน

๓.๓.๖ การฝึกอบรมบุคลากร (Big Data Training)

การฝึกอบรมบุคลากรด้านบิ๊กดาต้า ถือเป็นปัจจัยสำคัญที่ช่วยพัฒนาบุคลากรคอมพิวเตอร์ที่เกี่ยวข้องหรือนักวิเคราะห์ข้อมูลให้กับหน่วยงานด้านความมั่นคง เพื่อให้บุคลากรเหล่านี้สามารถปฏิบัติงานหรือทำงานกับระบบที่พัฒนาขึ้นมาได้ด้วยตนเองในอนาคต สำหรับแนวทางในการฝึกอบรม จะเน้นการฝึกปฏิบัติกับข้อมูลโจทย์ และระบบจริง โดยทีมผู้เชี่ยวชาญด้านบิ๊กดาต้าในระหว่างการพัฒนาระบบไปพร้อมๆ กัน ซึ่งเรียกการฝึกอบรมแบบนี้ว่า On-the-Job Training (OJT) ซึ่งต่างจากการฝึกอบรมเชิงปฏิบัติการทั่วไป (Workshop training) ที่มักจะใช้ระยะเวลาสั้นๆ ประมาณ ๒-๓ วันต่อหลักสูตร ซึ่งอาจจะไม่เพียงพอในการสร้างความรู้และความชำนาญให้กับผู้เข้ารับการอบรม โดยผู้เข้ารับการฝึกอบรมแบบ OJT จะต้องจัดทีมบิ๊กดาต้าเข้ามาทำงานจริงร่วมกับผู้ฝึกอบรม (ทีมพัฒนา) ดังแผนภาพที่ ๑๕



แผนภาพที่ ๑๕ กระบวนการทำงานบิ๊กดาต้าแบบ On-the-Job-Training (OJT)

แผนภาพที่ ๑๕ แสดงกระบวนการทำงานบิ๊กดาต้า (Big data lifecycle) โดยใช้การฝึกอบรมแบบ OJT ซึ่งผู้เข้ารับการฝึกอบรมจะต้องจัดทีมงานเข้ามาเรียนรู้และฝึกปฏิบัติร่วมกับทีมผู้เชี่ยวชาญอย่างน้อย ๔ ตำแหน่ง ได้แก่ หัวหน้าทีม (Team leader) ที่มีความรู้ความเข้าใจในโจทย์หรือข้อมูลที่จะทำ วิศวกรข้อมูล (Data engineer) ที่มีความรู้ด้าน IT และระบบฐานข้อมูล นักวิเคราะห์ข้อมูล (Data analyst) ที่มีความรู้ในการวิเคราะห์โจทย์และข้อมูล เพื่อนำไปทำรายงานผลการวิเคราะห์แบบ Dashboard และนักพัฒนาระบบ (Developer) ที่มีความรู้ในการเขียนโปรแกรมหรือพัฒนาแอปพลิเคชัน โดยแต่ละวงรอบจะใช้เวลาประมาณสองสัปดาห์และมีผลลัพธ์ที่ได้จากการทำงานในแต่ละรอบ กระบวนการนี้ จะทำแบบวนซ้ำไปเรื่อยๆ จนกว่างานที่ทำจะเสร็จสมบูรณ์ โดยหลักสูตรที่จะฝึกอบรมในโครงการนี้จะเน้นการปูพื้นฐานให้กับบุคลากรทุกด้าน จำนวน ๕ หลักสูตร ดังนี้

๓.๓.๕.๑ หลักสูตรบิ๊กดาต้าพื้นฐาน (Introduction to Big Data) เพื่อให้ผู้รับการอบรมมีความเข้าใจพื้นฐานระบบบิ๊กดาต้า กระบวนการทำงานของระบบบิ๊กดาต้า และการใช้ประโยชน์จากข้อมูลขนาดใหญ่ เนื้อหาการฝึกอบรมมีดังนี้

- ความสำคัญและแนวโน้มการใช้งานระบบบิ๊กดาต้า (Why Big data)
- แนะนำระบบบิ๊กดาต้า (Big data system)
- แนะนำบริการพื้นฐานในระบบบิ๊กดาต้า (Big data foundation services)
- กระบวนการทำงานในระบบบิ๊กดาต้า (Big data processes)
- เครื่องมือที่เกี่ยวข้องกับการทำงาน (Cloudera, Hue, Talend, Tableau)
- การใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big data use cases)

๓.๓.๕.๒ หลักสูตรผู้ดูแลระบบบิ๊กดาต้าแพลตฟอร์ม (Big data platform administration) เพื่อให้ผู้รับการอบรมเข้าใจ หลักการออกแบบและพัฒนาระบบบิ๊กดาต้า สามารถใช้งานบิ๊กดาต้าแพลตฟอร์ม รวมทั้งการบริหารจัดการทรัพยากร บริการ และผู้ใช้ในระบบได้ เนื้อหาการฝึกอบรมมีดังนี้

- ระบบ Infrastructure และการเลือกใช้
- ระบบบิ๊กดาต้า (Big data system)
- บริการพื้นฐานในระบบบิ๊กดาต้า (Big data foundation services)
- การบริหารจัดการผู้ใช้ในระบบบิ๊กดาต้า (User management)
- การตรวจสอบระบบและการบริหารจัดการระบบด้วย Cloudera Manager
- การสำรองและกู้คืนข้อมูล (Backup and Recovery)

๓.๓.๕.๓ หลักสูตรการบริหารจัดการข้อมูลบิ๊กดาต้า (Big data management) เพื่อให้ผู้รับการอบรมเข้าใจ ขั้นตอนการเตรียมข้อมูล และสามารถใช้งานเครื่องมือบริหารจัดการข้อมูลขั้นต้น ได้แก่ การนำเข้าข้อมูล การตรวจสอบคุณภาพข้อมูล การทำความสะอาดข้อมูล การปกปิดข้อมูล และการทำ ETL รวม ทั้งฝึกให้ใช้งาน Query editor สำหรับจัดการกับข้อมูลด้วยภาษา SQL บนระบบฐานข้อมูลขนาดใหญ่ได้ เนื้อ หาการฝึกอบรมมีดังนี้

- พื้นฐานและความสำคัญของการบริหารจัดการข้อมูล
- การบริหารจัดการข้อมูล ด้วย SQL และ เครื่องมือพื้นฐานด้านบิ๊กดาต้า (Sqoop)
- การนำเข้าข้อมูล (Data ingestion)
- การตรวจสอบคุณภาพข้อมูล (Data quality)
- การทำความสะอาดข้อมูล (Data cleansing)
- การปกปิดข้อมูล (Data masking)
- การดัดแปลง และจัดเก็บข้อมูลบนบิ๊กดาต้าแพลตฟอร์ม ตามกระบวนการ ETL (Extract-Transform-Load) ด้วยเครื่องมือ ETL
- การทำ ETL และ ELT (Extract-Load-Transform) เพื่อจัดเก็บในคลังข้อมูล (Data warehouse)
- การจัดการและจัดตารางงาน ELT job และ Workflow (Job scheduling)
- การให้บริการข้อมูล (Data services)

๓.๓.๕.๔ หลักสูตรการวิเคราะห์ข้อมูลและทำรายงาน (Data analytics and visualization) เพื่อให้ผู้ใช้มีความเข้าใจพื้นฐานในการวิเคราะห์ข้อมูลและทำรายงาน การใช้เครื่องมือในการสร้าง Dashboard เนื้อหาการฝึกอบรมมีดังนี้

- แนะนำการวิเคราะห์ข้อมูล (Introduction to data analytic)
- แนะนำเกี่ยวกับการแสดงผลด้วยภาพ (Introduction to data visualization)
- แนะนำการใช้เครื่องมือธุรกิจอัจฉริยะ (Introduction to BI tool)
- ใช้โปรแกรม Tableau สร้าง Dashboard
- การเชื่อมต่อแหล่งข้อมูลประเภทต่างๆ เช่น csv file, SQL, Oracle, MySQL และ Hadoop
- สร้าง Dashboard จากข้อมูลของหน่วยงาน
- การแบ่งปัน Dashboard ผ่าน Tableau Public

๓.๓.๕.๕ หลักสูตรบิ๊กดาต้าสำหรับผู้บริหาร (Big data for executive) เพื่อให้ผู้บริหารเข้าใจโครงสร้างบุคลากรด้านบิ๊กดาต้า แนวทางการทำระบบบิ๊กดาต้าในองค์กร รวมทั้งการนำบิ๊กดาต้ามาสนับสนุนการวางแผนและตัดสินใจของผู้บริหารได้อย่างรวดเร็วและแม่นยำ เนื้อหาการฝึกอบรมมีดังนี้

- ระบบบิ๊กดาต้า In general, บุคลากรด้านบิ๊กดาต้า, อนาคตและทิศทาง
- การธรรมาภิบาล Data Governance
- กฎหมายเกี่ยวกับบิ๊กดาต้า
- การนำระบบบิ๊กดาต้า มาใช้ประโยชน์ และสนับสนุนด้านการวางแผนและตัดสินใจ

๓.๔ สรุป กิจกรรม ผลลัพธ์ และงบประมาณของโครงการ

โครงการพัฒนาระบบแพลตฟอร์มพื้นฐาน (Quickwin Big Data Platform) ระยะที่ ๑ ในปีที่ ๑ ระยะเวลาดำเนินการ ๑๒ เดือน สามารถแยกกิจกรรมออกเป็นส่วนๆ พร้อมผลลัพธ์ที่ได้ และประมาณการกรอบวงเงินงบประมาณ ดังนี้

กิจกรรม	ผลลัพธ์	งบประมาณ (ล้านบาท)
๑. การวิเคราะห์และออกแบบระบบ		๙
๑.๑ จัดประชุมและสัมภาษณ์	รายงานการประชุมและสัมภาษณ์	๑
๑.๒ วิเคราะห์โจทย์ ข้อมูล และระบบ	รายงานผลการวิเคราะห์	๑
๑.๓ จัดทำมาตรฐานร่วม	เอกสารมาตรฐานร่วม	๕
๑.๔ จัดทำแผนแม่บทบิ๊กดาต้า	เอกสารแผนแม่บท	๒
๒. พัฒนาระบบบิ๊กดาต้าแพลตฟอร์ม		๒๓
๒.๑ จัดหาเครื่องแม่ข่ายและซอฟต์แวร์	เครื่องแม่ข่ายและซอฟต์แวร์	๘
๒.๒ พัฒนาระบบบริหารจัดการบิ๊กดาต้า	ระบบบริหารจัดการบิ๊กดาต้า	๕
๒.๓ พัฒนาระบบรักษาความปลอดภัย	ระบบรักษาความปลอดภัย	๕
๒.๔ พัฒนาระบบบริหารจัดการทรัพยากร	ระบบบริหารจัดการทรัพยากร	๒
๒.๕ พัฒนาระบบบริหารจัดการผู้ใช้	ระบบบริหารจัดการผู้ใช้	๒
๒.๖ จัดทำเอกสารและคู่มือการใช้งาน	เอกสารและคู่มือการใช้ระบบบิ๊กดาต้าแพลตฟอร์ม	๑
๓. พัฒนาระบบบริหารจัดการข้อมูล		๒๐
๓.๑ พัฒนาระบบนำเข้าและเชื่อมโยงข้อมูล	ระบบนำเข้าและเชื่อมโยงข้อมูล	๔

๓.๒ พัฒนาระบบตรวจสอบคุณภาพข้อมูล	ระบบตรวจสอบคุณภาพข้อมูล	๓
๓.๓ พัฒนาระบบทำความสะอาดข้อมูล	ระบบทำความสะอาดข้อมูล	๓
๓.๔ พัฒนาระบบ ETL	ระบบ ETL	๓
๓.๕ พัฒนาระบบฐานข้อมูลบิ๊กดาต้า	ระบบฐานข้อมูลบิ๊กดาต้า	๓
๓.๖ พัฒนาระบบให้บริการข้อมูล	ระบบให้บริการข้อมูล	๓
๓.๗ จัดทำเอกสารและคู่มือการใช้งาน	เอกสารและคู่มือการใช้ระบบ บริหารจัดการข้อมูล	๑
๔. พัฒนาระบบวิเคราะห์และทำรายงาน		๑๖
๔.๑ พัฒนาระบบวิเคราะห์ข้อมูล	ระบบวิเคราะห์ข้อมูล	๓
๔.๒ พัฒนาระบบทำรายงาน	ระบบทำรายงาน	๓
๔.๓ พัฒนาระบบวิเคราะห์และรายงานสถานการณ์สามจังหวัดชายแดนภาคใต้	ระบบวิเคราะห์และรายงานสถานการณ์สามจังหวัด ชายแดนภาคใต้	๓
๔.๔ พัฒนาระบบวิเคราะห์และติดตามอาชญากรรมข้ามชาติและการก่อการร้าย	ระบบวิเคราะห์และติดตามอาชญากรรมข้ามชาติ และการก่อการร้าย	๓
๔.๕ พัฒนาระบบวิเคราะห์สถานการณ์ป้องกันและแก้ไขปัญหาภัยน้ำท่วม	ระบบวิเคราะห์สถานการณ์ป้องกันและแก้ไขปัญหาภัยน้ำท่วม	๓
๔.๖ จัดทำเอกสารและคู่มือการใช้งาน	เอกสารและคู่มือการใช้ระบบ บริหารจัดการข้อมูล	๑
๕. พัฒนาระบบวิเคราะห์และแจ้งเตือนภัย		๑๘
๕.๑ พัฒนาระบบ war room ความมั่นคง	ระบบ war room ความมั่นคง	๑๐
๕.๒ พัฒนาระบบแจ้งเตือนภัยแบบ real-time	ระบบแจ้งเตือนภัยแบบ real-time	๔
๕.๓ พัฒนาระบบ Mobile app	ระบบ Mobile app ความมั่นคง	๔
๖. การฝึกอบรมบิ๊กดาต้า		๑๐
๖.๑ หลักสูตรพื้นฐานบิ๊กดาต้า	ผู้สำเร็จหลักสูตรพื้นฐานบิ๊กดาต้า	๒

๖.๒ หลักสูตร big data admin	ผู้สำเร็จหลักสูตร big data admin	๒
๖.๓ หลักสูตร data engineer	ผู้สำเร็จหลักสูตร data engineer	๒
๖.๔ หลักสูตร data analytics and visualization	ผู้สำเร็จหลักสูตร data analytics and visualization	๒
๖.๕ หลักสูตรบิ๊กดาต้าสำหรับผู้บริหาร	ผู้สำเร็จหลักสูตรบิ๊กดาต้าสำหรับผู้บริหาร	๒
รวมทั้งสิ้น		๙๖

บทที่ ๔ การพัฒนาบิ๊กดาต้าด้านความมั่นคงระยะที่ ๒ ปีที่ ๒

โครงการพัฒนาบิ๊กดาต้าด้านความมั่นคงระยะที่ ๒ ปีที่ ๒ จะเป็นการพัฒนาและต่อยอดโครงการพัฒนาบิ๊กด้าด้านความมั่นคง สืบเนื่องจากการดำเนินงานในระยะที่ ๑ โดยในระยะที่ ๒ นี้ จะมีการพัฒนาระบบให้ครอบคลุมทั้ง ๔ ด้าน ตั้งแต่ระบบบิ๊กดาต้าแพลตฟอร์ม ระบบบริหารจัดการและธรรมาภิบาลข้อมูล ระบบวิเคราะห์และใช้ประโยชน์จากข้อมูล จนถึงการพัฒนาบุคลากรด้านบิ๊กดาต้า ซึ่งในระยะนี้ จะเน้นการยกระดับระบบบิ๊กดาต้าแพลตฟอร์มให้เป็นบิ๊กดาต้าแพลตฟอร์มระดับองค์กร (Enterprise Big Data Platform) พร้อมระบบแพลตฟอร์มสำรอง เพื่อให้ระบบมีประสิทธิภาพและมีความน่าเชื่อถือ โดยมีรายละเอียดโครงการ ดังนี้

๔.๑ วัตถุประสงค์โครงการ

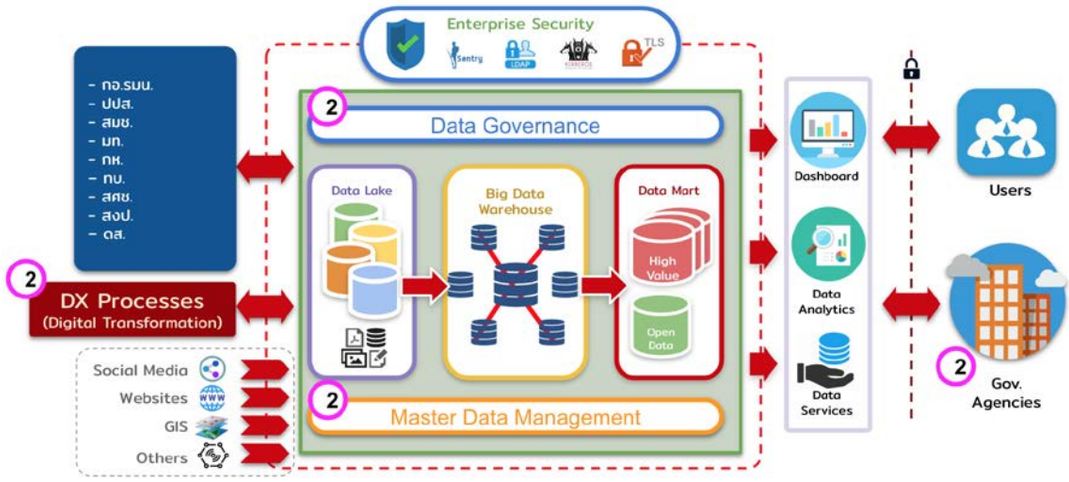
๔.๑.๑ เพื่อพัฒนาระบบบิ๊กดาต้า ให้มีขีดความสามารถและความน่าเชื่อถือสูง เป็นแพลตฟอร์มระดับองค์กร รวมทั้งมีแพลตฟอร์มสำรอง ในการจัดเก็บและประมวลผลข้อมูล เมื่อแพลตฟอร์มหลักขัดข้อง

๔.๑.๒ เพื่อพัฒนาให้ระบบฐานข้อมูลในบิ๊กดาต้า เป็นระบบฐานข้อมูลกลางที่สามารถนำไปเชื่อมโยงกับฐานข้อมูลของหน่วยงานต่างๆ ได้ ทำให้การเข้าถึงข้อมูลหรือการใช้ข้อมูลร่วมกัน มีความสะดวกและรวดเร็วมากยิ่งขึ้น

๔.๑.๓ เพื่อให้ข้อมูลด้านความมั่นคงที่มีอยู่ เป็นข้อมูลที่ได้รับการยืนยันกรรมสิทธิ์ ว่าเป็นข้อมูลขององค์กรโดยแท้จริง ด้วยระบบการธรรมาภิบาลข้อมูล (Data governance)

๔.๒ รายละเอียดการพัฒนาระบบตามแผนการดำเนินการในระยะที่ ๒ ปีที่ ๒

ในระยะที่ ๒ โครงการพัฒนาด้านบิ๊กดาต้าแพลตฟอร์ม จะเป็นการพัฒนาระบบให้เป็นระดับองค์กร (Enterprise big data platform) เพื่อให้ระบบมีขีดความสามารถในด้านอื่นๆ มากขึ้น เช่น ให้สามารถรองรับการนำเข้าข้อมูลแบบ real-time ได้อย่างมีประสิทธิภาพ และมีระบบการรักษาความปลอดภัยอย่างเต็มรูปแบบ มีการเพิ่มการเชื่อมโยงและแลกข้อมูลจากหน่วยงานต่างๆ มากขึ้น พร้อมกับการรองรับกับการนำเข้าข้อมูลใหม่ ที่เป็นผลผลิตจากโครงการต่างๆ ที่เกี่ยวข้องกับการเปลี่ยนองค์กรให้เป็นดิจิทัล (Digital transformation) มีระบบการธรรมมาภิบาลข้อมูล (Data governance) ที่ได้มาตรฐาน มีระบบการจัดการข้อมูลหลัก (Master data management) รวมทั้งเพิ่มบิ๊กดาต้าแพลตฟอร์มสำรอง (DR-site) ที่เป็นบิ๊กดาต้าแพลตฟอร์มสำรอง เพื่อให้ระบบงานสามารถทำงานได้อย่างต่อเนื่อง ในกรณีแพลตฟอร์มหลักจะมีปัญหาข้อขัดข้อง หรือข้อมูลหลักสูญหาย ในส่วนของระบบบริหารจัดการข้อมูลจะเพิ่มบริการที่หลากหลายมากขึ้น

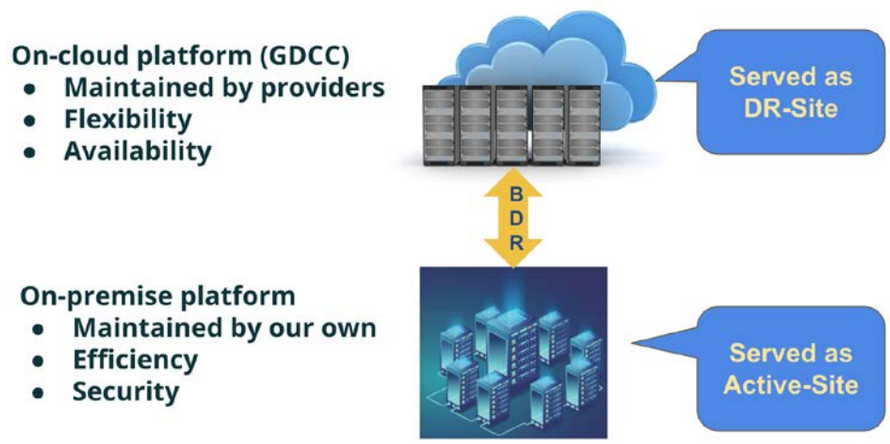


แผนภาพที่ ๑๖ แสดงสถาปัตยกรรม Enterprise Big Data Platform ระยะที่ ๒ ปีที่ ๒

แผนภาพที่ ๑๖ แสดงภาพสถาปัตยกรรมระบบบิ๊กดาต้าแพลตฟอร์มระดับองค์กร (Enterprise big data platform) ที่มีส่วนบริหารและกำกับดูแลการใช้ข้อมูลในองค์กรอย่างสมบูรณ์ ได้แก่ Master data management และ Data governance เพื่อให้การแลกเปลี่ยนข้อมูลระหว่างองค์กรเป็นไปตามมาตรฐานของภาครัฐ นอกจากนี้ยังเพิ่มระบบการแปลงข้อมูลให้เป็นดิจิทัล (Digital Transformation) เพื่อนำข้อมูลในรูปแบบเอกสารทั่วไปมาแปลงให้เป็นข้อมูลดิจิทัล ก่อนจะนำเข้ามาสู่กระบวนการวิเคราะห์และทำรายงาน และมีบริการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานราชการต่างๆ ผ่านระบบ Data services ตามลำดับ

๔.๒.๑ โครงสร้างพื้นฐานระบบบิ๊กดาต้า (Big data infrastructure)

ในส่วนของโครงสร้างพื้นฐาน (Infrastructure) ได้มีการออกแบบให้ผสมผสานข้อดีและลดข้อเสียของระบบโครงสร้างแบบ on-premise platform และแบบ on-cloud platform โดยมีการนำระบบทั้งสอง มาใช้ร่วมกันเป็นระบบแบบ Hybrid ดังแผนภาพที่ ๑๗



แผนภาพที่ ๑๗ ระบบโครงสร้างพื้นฐานแบบ Hybrid platform

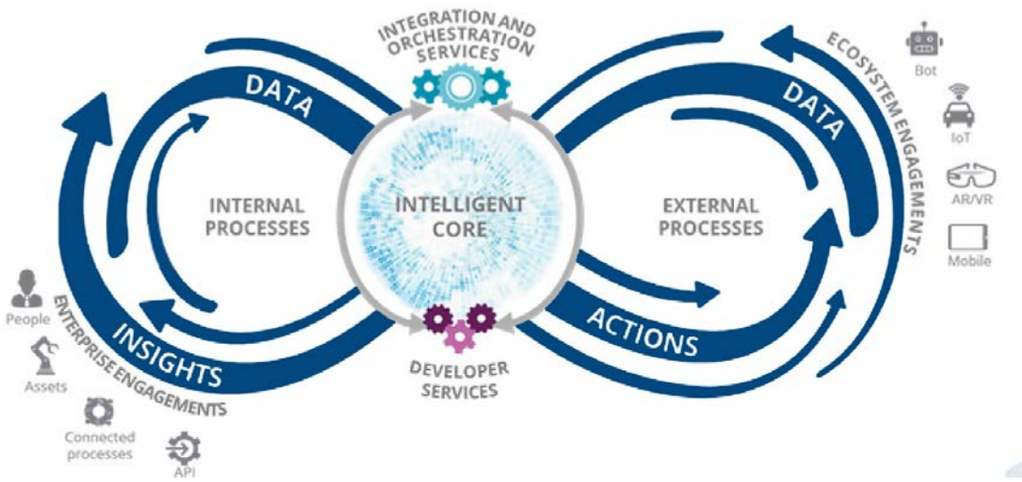
แผนภาพที่ ๑๗ เป็นการนำโครงสร้างพื้นฐานแบบ Hybrid มาใช้ทำบิ๊กดาต้าแพลตฟอร์ม โดยใช้โครงสร้างแบบ on-premise platform และแบบ on-cloud platform มาใช้ร่วมกัน โดยโครงสร้างแบบ on-premise จะมีประสิทธิภาพ (Efficiency) และความปลอดภัย (Security) สูงกว่า เนื่องจากระบบจะทำงานบนฮาร์ดแวร์โดยตรง ทำให้สามารถใช้ขีดความสามารถของหน่วยประมวลผล (Processing unit) หน่วยจัดเก็บข้อมูล (Storage) และหน่วยรับส่งข้อมูล (I/O unit) ในระบบได้อย่างเต็มที่ นอกจากนี้ระบบยังมีความปลอดภัยสูงเพราะฮาร์ดแวร์ อุปกรณ์ และระบบปฏิบัติการ จะถูกควบคุมและดูแลโดยเจ้าหน้าที่ขององค์กร จึงเหมาะสมที่จะใช้เป็นแพลตฟอร์มหลักในการทำงานของระบบ

ส่วนระบบแบบ on-cloud จะมีความยืดหยุ่น (Flexibility) ในการเพิ่มหรือลดทรัพยากรในระบบมากกว่า และมีความน่าเชื่อถือหรือความพร้อมใช้งานของข้อมูล (Availability) สูง เนื่องจากระบบคลาวด์ในปัจจุบันจะใช้เทคโนโลยี Hyper Converged Infrastructure (HCI) ที่มีซอฟต์แวร์บริหารจัดการในการปรับทรัพยากรและบริการพื้นฐานของระบบโดยไม่กระทบกับการใช้งานของผู้ใช้งาน อย่างไรก็ตามระบบปฏิบัติการของผู้ใช้ในระบบคลาวด์ จะไม่ได้ติดต่อกับฮาร์ดแวร์โดยตรง ทำให้เสียเวลาในการเคลื่อนย้ายข้อมูล ในระบบเครือข่ายมากกว่า จึงทำให้มีประสิทธิภาพต่ำกว่าโครงสร้างแบบ On-premise Platform นอกจากนี้ผู้ดูแลระบบยังเป็นของผู้ให้บริการคลาวด์เอง การรักษาความปลอดภัยในระดับล่างสุดจึงขึ้นอยู่กับผู้ให้บริการคลาวด์ ดังนั้นแพลต ฟอร์มนี้จึงเหมาะที่จะใช้เป็นระบบสำรองมากกว่า โดยระบบทั้งสองจะมีการเชื่อมโยงปรับปรุงข้อมูล (Data synchronization) ระหว่างกันอยู่ตลอดเวลา หากระบบหลักมีปัญหาขัดข้อง เราสามารถสลับไปทำงานบนระบบสำรองในคลาวด์ได้ทันที ก่อนที่จะดำเนินการกู้คืน (Recovery) ระบบหลัก และกลับมาทำงานต่อในระบบหลักตามเดิม

นอกจากนั้น ในส่วนของ data center ซึ่งเป็นสถานที่ติดตั้งเครื่องแม่ข่ายทั้งแบบ on-premise และ on-cloud จำเป็นต้องมีมาตรฐานที่สูง ทั้งความน่าเชื่อถือและความปลอดภัยของระบบ โดยในปัจจุบัน data center ในประเทศที่ได้รับมาตรฐานสูงสุดได้แก่ ระดับ TSI Level 3 หรือ tier 3 ซึ่งเป็น data center ที่มีระบบจ่ายไฟและระบบให้ความเย็นสองแหล่ง (Redundant power and cooling systems) ซึ่งทำให้ระบบสามารถทำงานต่อไปได้หากระบบไฟหรือระบบทำความเย็นระบบใดระบบหนึ่งชำรุด อีกส่วนสำคัญที่ควรมีควบคู่ไปกับความน่าเชื่อถือของระบบคือ ระบบรักษาความปลอดภัยซึ่งจำเป็นต้องมีศูนย์ปฏิบัติการด้านความปลอดภัย หรือ SOC (Security Operation Center) ที่ได้รับมาตรฐานสากล ได้แก่ ISO 270001 เป็นต้น ซึ่งมาตรฐานนี้จะกำหนดให้ ศูนย์ปฏิบัติการต้องมีบุคลากรที่มีความเชี่ยวชาญตรวจสอบระบบตลอด ๒๔ ชั่วโมง ทำให้ผู้ใช้มีความมั่นใจในการตรวจสอบภัยคุกคามต่อระบบมากยิ่งขึ้น

๔.๒.๒ Digital Transformation

การปฏิรูปองค์กรให้เป็นดิจิทัล หรือ Digital Transformation (DX) เป็นหนึ่งในนโยบายหลักของรัฐบาลในการปฏิรูปประเทศให้เป็น Thailand 4.0 ซึ่งเป็นการนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานเป็นหลัก และมีการใช้ประโยชน์จากข้อมูลอย่างเต็มรูปแบบ ซึ่งในอนาคตจะส่งผลให้สำนักงานสภาความมั่นคงแห่งชาติเกิดโครงการในการพัฒนาระบบสารสนเทศเพื่อการปฏิบัติภารกิจด้านความมั่นคงต่างๆมากมาย ซึ่งจะมาพร้อมกับการผลิตจำนวนข้อมูลต่างๆมากมายมหาศาลเช่นกัน ซึ่งจำเป็นอย่างยิ่งที่จะต้องมีระบบบิ๊กดาต้าแพลตฟอร์มที่มีประสิทธิภาพสูงในการรองรับการจัดเก็บ ประมวลผล และวิเคราะห์ข้อมูลต่างๆให้เกิดการใช้ประโยชน์จากข้อมูลในการดูแลรักษาความมั่นคงของประเทศในทุกมิติ



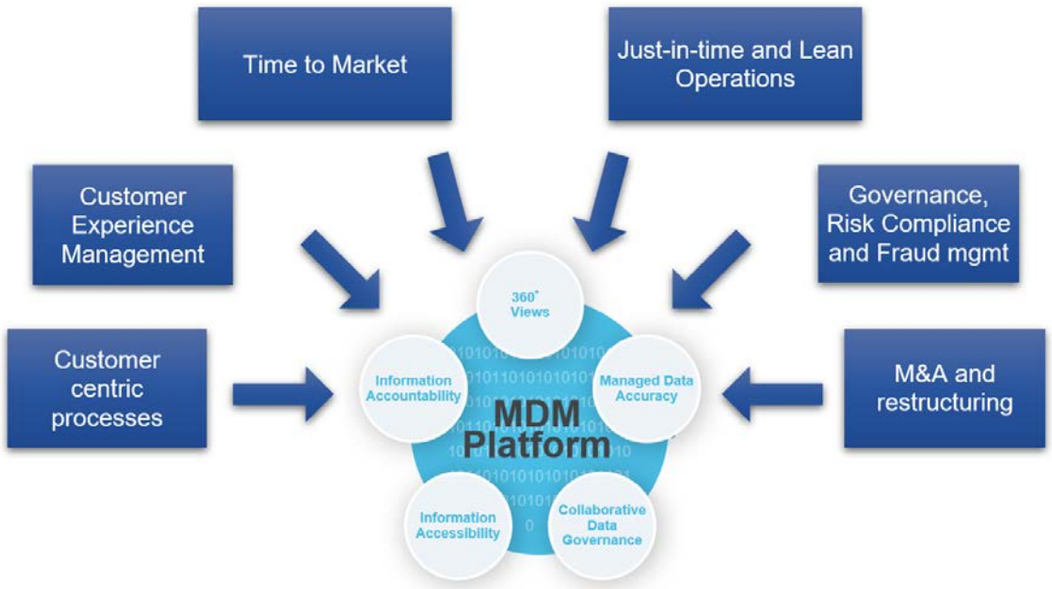
แผนภาพที่ ๑๘ ตัวอย่างกระบวนการ Digital Transformation หรือ DX
ที่มา: IDC 2018

โดยทั่วไปกระบวนการ Digital transformation (DX) ดังแสดงในแผนภาพที่ ๑๘ จะมีระบบ Intelligent Core เป็นแกนกลางซึ่งทำหน้าที่ในการรวบรวม จัดเก็บ ประมวลผล วิเคราะห์และให้บริการด้านข้อมูล (Data) ต่างๆ แกน Intelligent Core จะทำหน้าที่สร้างข้อมูลเชิงลึก (Insights) หรือผลการวิเคราะห์ที่มีประโยชน์ต่างๆ เพื่อเอาไปใช้ประโยชน์ให้กับธุรกิจและองค์กร ให้เกิดการใช้ประโยชน์ในการขับเคลื่อนองค์กร (Enterprise engagements) เพื่อให้คนในองค์กรนำไปใช้ประโยชน์ หรือเปลี่ยนข้อมูลที่มีค่าให้เป็นสินทรัพย์ (Assets) และให้ระบบภายในต่างๆ (Process) ได้ใช้ หรือให้บริการข้อมูลในรูปแบบของ API เป็นต้น จากการปฏิบัติงานของหน่วยงานภายใน องค์กรก็จะผลิตข้อมูลชุดใหม่ๆ อย่างไม่มีที่สิ้นสุด เพื่อป้อนกลับเข้าระบบ Intelligent Core ใหม่เพื่อใช้ในการทำกิจกรรมหรือ Action ในการปฏิบัติงานกับองค์กร หน่วยงานและระบบภายนอกต่างๆ ซึ่งอาจจะประกอบไปด้วยเครื่องจักร (Machines) หุ่นยนต์ (Bot) เครื่อง Sensors หรือ IoT และ Application ต่างๆ ซึ่งกิจกรรมต่างๆจากภายนอกองค์กร ก็จะผลิต Data ชุดใหม่ส่งกลับเข้าสู่แกน Intelligent core อีกครั้งกระบวนการและกิจกรรมต่างๆเหล่านี้ก็จะวนไปเป็นวัฏจักรโดยไม่มีที่สิ้นสุด โครงการด้าน Digital Transformation ต่างๆของสำนักงานสภาความมั่นคงแห่งชาติสามารถที่จะเริ่มในโครงการระยะที่ ๒ โดยโครง การที่เกี่ยวข้องกับงานด้าน Digital Transofrmation ต้องตอบสนองตามยุทธศาสตร์และภารกิจของสำนักงานสภาความมั่นคงแห่งชาติเป็นหลัก

๔.๒.๓ Master Data Management

ระบบ Master Data Management เป็นระบบสำหรับจัดการข้อมูลหลักที่จะเป็นแหล่งข้อมูลจริงหนึ่งเดียว (Single source of truth) ที่เชื่อถือได้ (Trusted data) ผ่านการตรวจสอบคุณภาพและความถูกต้องและถือเป็นแหล่งข้อมูลอ้างอิงของทุกๆหน่วยงานและผู้ใช้ข้อมูล ระบบบริหารจัดการข้อมูลหลักมีความจำเป็นอย่างยิ่งในการบริหารจัดการข้อมูลจากหลากหลายแหล่งที่มีรูปแบบโครงสร้างที่แตกต่างกัน ซ้ำซ้อนกัน ข้อมูลที่มากมายเหล่านี้จะถูกรวบรวมมาจัดเก็บเป็นแหล่งข้อมูลแหล่งเดียวที่สามารถบริหารจัดการได้แบบรวมศูนย์ ซึ่งมีประโยชน์ในการสร้างความมั่นใจในเรื่องคุณภาพข้อมูล การควบคุมการเข้าถึงของข้อมูลของผู้ใช้ข้อมูล

ต่างๆ (Data consumer) ซึ่งเป็นหัวใจของการธรรมมาภิบาลข้อมูล จะเป็นเครื่องมือหลักสำหรับผู้กำกับดูแลข้อมูลและเจ้าของข้อมูลในการบริหารจัดการตรวจสอบความถูกต้องและทำความสะอาดข้อมูล และสามารถเห็นภาพ ของข้อมูลทั้งหมดได้จากที่เดียว ดังแสดงในแผนภาพที่ ๑๙ ตัวอย่างความความสำคัญของระบบ Master Data Management หรือ MDM



แผนภาพที่ ๑๙ ความสำคัญของระบบ Master Data Management (MDM)
ที่มา: Talend.com

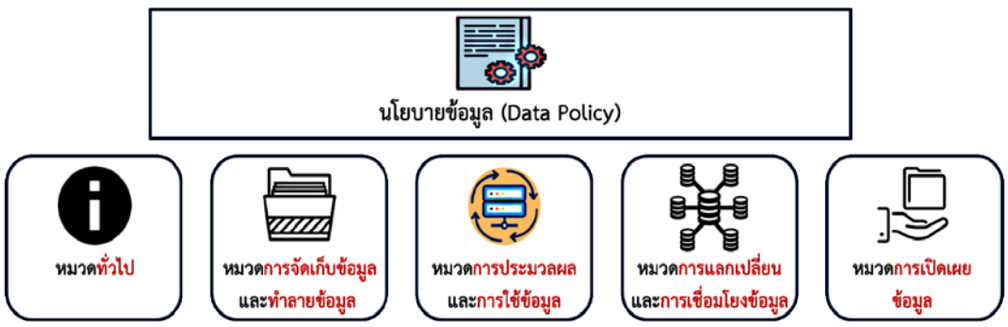
๔.๒.๔ Data Governance

การธรรมมาภิบาลข้อมูล (Data governance) เป็นสิ่งที่สำคัญในยุคที่ข้อมูลข่าวสารสามารถเข้าถึงได้จากทุกที่ ตลอดเวลาและสะดวก โดยเฉพาะในหน่วยงานที่มีระบบบิ๊กดาต้าแพลตฟอร์มที่ใช้จัดเก็บและประมวลผลข้อมูลขนาดใหญ่ การรักษาความปลอดภัย (Data security) และการรักษาความลับข้อมูลส่วนตัว (Data privacy) ถือว่าเป็นสิ่งที่ต้องปฏิบัติตามอย่างเคร่งครัดและไม่สามารถหลีกเลี่ยงได้อีกต่อไป ทั้งนี้สำนักงานสภาความมั่นคงแห่งชาติมีความจำเป็นที่จะต้องมีระบบจัดการและบริหารข้อมูลที่ได้มาตรฐาน มีการจัดทำนโยบายด้านการรักษาความปลอดภัยข้อมูลและมีบุคลากรที่มีหน้าที่รับผิดชอบ และกำกับดูแลด้านนี้โดยตรง ทั้งนี้เพื่อขจัดอุปสรรคด้านกฎหมายในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน มีการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลและข้อมูลที่ต้องปกปิด มีการกำหนดมาตรฐานเพื่อการเชื่อมโยงและปรับปรุงข้อมูล และมีการขับ เคลื่อนโครงการต่างๆ ที่มีความสำคัญ โดยให้การสนับสนุนทางงบประมาณ องค์ความรู้และบุคลากร

๔.๒.๔.๑ การจัดสร้างสภาพแวดล้อมของการกำกับดูข้อมูล (Data Governance Environment) เพื่อให้การดำเนินการต่อข้อมูลด้านความมั่นคง สามารถผ่านมาตรฐานการธรรมมาภิบาลข้อมูลของชาติและสามารถนำพาองค์กรให้เป็นองค์กรที่ขับเคลื่อนด้วยข้อมูลอย่างเต็มรูปแบบ มีความจำเป็นอย่างยิ่งที่จะต้องมีนโยบายเพื่อสร้างสภาพแวดล้อมของการกำกับดูแลข้อมูล ซึ่งการสร้างสภาพแวดล้อมจะเริ่ม

ต้นที่การกำหนด กฎระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล ซึ่งจะต้องอยู่ในกรอบที่กฎหมายกำหนด เป็นการสร้างหรือปรับปรุงระบบภายในให้มีการกำกับดูแลข้อมูล และจะต้องมีการพิจารณาตามประเด็นหลัก ๆ ที่เกี่ยวข้องกับกฎหมาย เช่น การเปิดเผยข้อมูล การแลกเปลี่ยนข้อมูล การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความลับ เป็นต้น

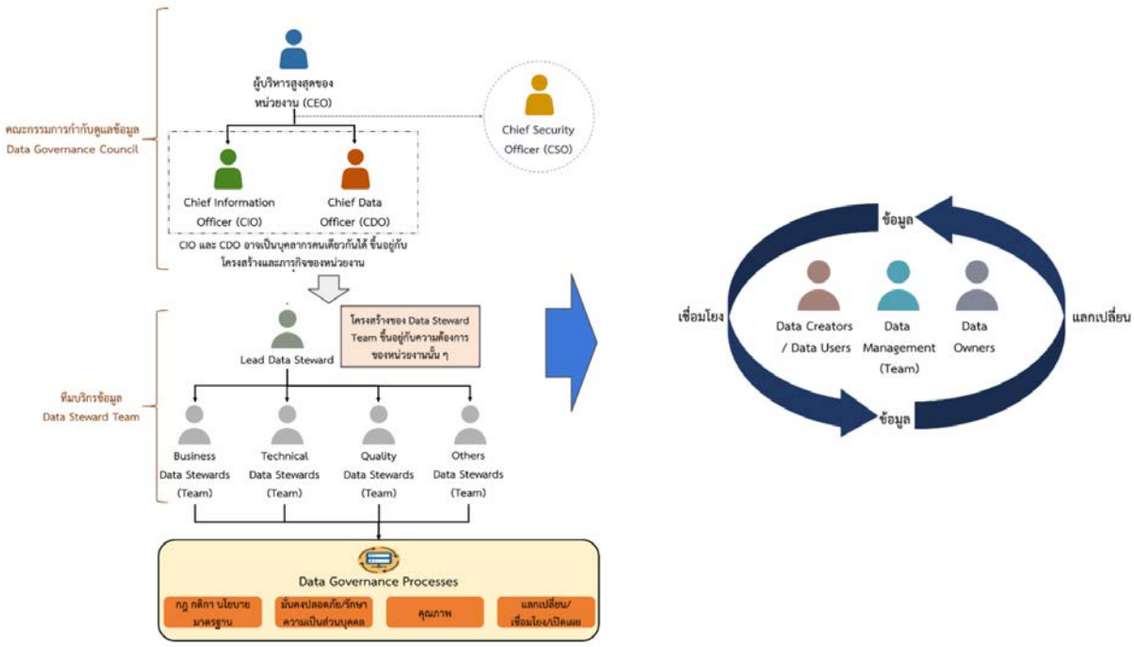
๔.๒.๔.๒ การสร้างกฎเกณฑ์ของข้อมูลและนโยบายข้อมูล ตามเอกสารกรอบการกำกับดูแลข้อมูล **(Data Governance Framework)** ซึ่งกำหนดโดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ได้กำหนดไว้ว่า การสร้างกฎเกณฑ์ของข้อมูลและนโยบายข้อมูล เป็นส่วนหนึ่งของการสร้างสภาพแวดล้อมของการกำกับดูแลข้อมูล ประกอบด้วย ๑) การกำหนดนิยามข้อมูล **(Data Definition)** ๒) การจัดหมวดหมู่ของข้อมูล **(Data Category)** เช่น ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และข้อมูลสาธารณะ เป็นต้น ๓) การกำหนดเมทาดาตา **(Metadata)** เพื่อใช้เป็นข้อมูลสำหรับอธิบายข้อมูล ๔) การกำหนดบัญชีข้อมูล **(Data Catalog)** หรือ รายการชุดข้อมูลที่หน่วยงานถือครองหรือบริหารจัดการ และ ๕) การกำหนดกฎเกณฑ์ข้อมูล **(Data rules)** ซึ่งจะใช้สำหรับการบังคับใช้ให้ปฏิบัติตามนโยบายและมาตรฐานที่เกี่ยวข้องกับข้อมูล ที่จะอธิบายถึงข้อควรปฏิบัติและข้อห้ามปฏิบัติ ดังแผนภาพที่ ๒๐ แสดงตัวอย่างนโยบายข้อมูลเพื่อใช้กำหนดข้อควรปฏิบัติซึ่งแบ่งเป็นหมวดหมู่ที่สอดคล้องกับข้อบังคับและข้อกฎหมาย



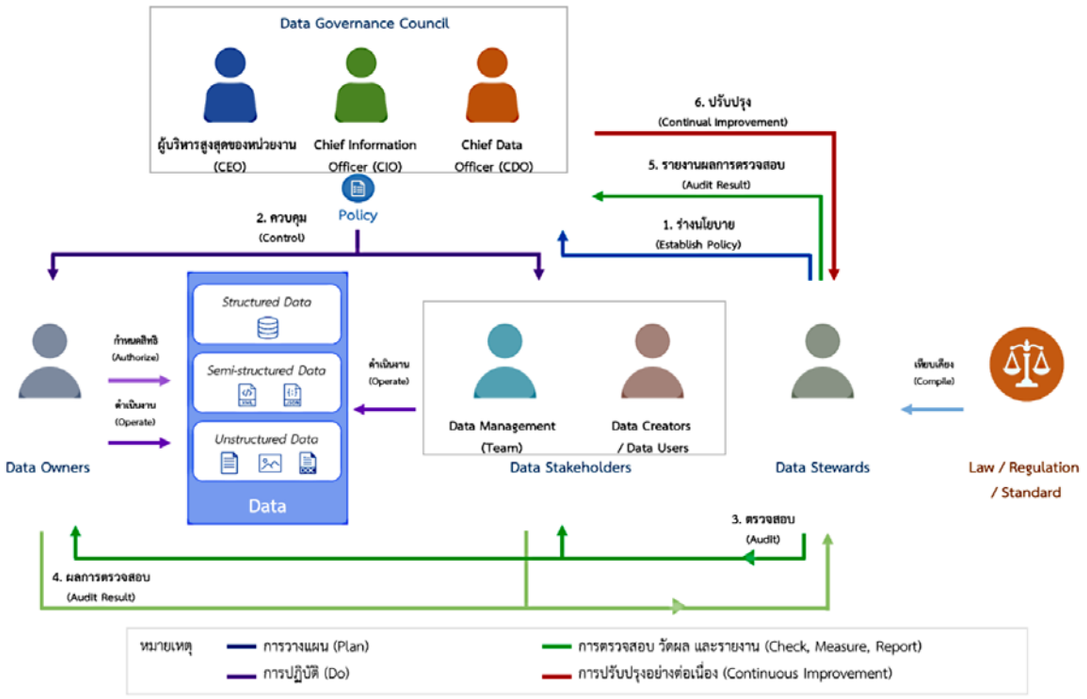
แผนภาพที่ ๒๐ ตัวอย่างมาตรฐานข้อมูลและมาตรฐานการปฏิบัติ
ที่มา: เอกสาร กรอบการกำกับดูแลข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๔.๒.๔.๓ การกำหนดมาตรฐานข้อมูล (Data Standards) การกำหนดมาตรฐานข้อมูลเป็นกลไลอย่างหนึ่งในการกำกับดูแลข้อมูล เพื่อสร้างความเข้าใจที่ตรงกันของหน่วยงานภายในและภายนอก และลดความหลากหลายของการปฏิบัติ ซึ่งกิจกรรมต่างๆ ประกอบด้วย การกำหนดมาตรฐานเมทาดาตา (Metadata Standard) มาตรฐานชุดข้อมูล (Datasets Standard) และมาตรฐานการจัดชั้นความลับของข้อมูล (Data Classification Standard) เป็นต้น

๔.๒.๔.๔ การปรับเปลี่ยนโครงสร้างด้านบุคลากรกำกับดูแลข้อมูล นอกจากการพิจารณากำหนดมาตรฐานข้อมูลและมาตรฐานการปฏิบัติต่างๆแล้ว การปรับเปลี่ยนโครงสร้างด้านบุคลากรให้รองรับการกำกับดูแลข้อมูลเป็นสิ่งที่จำเป็นเช่นกัน DGA ได้กำหนดและแนะนำการแบ่งผู้ที่เกี่ยวข้องที่มีหน้าที่กำกับดูแลข้อมูลขององค์กร ซึ่งประกอบไปด้วย คณะกรรมการกำกับดูแลข้อมูล **(Data governance concil)** ทีมบริกรข้อมูล **(Data steward team)** และผู้มีส่วนได้ส่วนเสียกับข้อมูล **(Data stakeholders)** ดังแสดงในแผนภาพที่ ๒๑ และ ๒๒ ตัวอย่างโครงสร้างและการปฏิบัติงานของบุคคลากรกำกับดูแลข้อมูลของสำนักงานสภาความมั่นคงแห่งชาติ ตั้งแต่ผู้บริหารข้อมูลระดับสูง **(Chief Data Officer** หรือ **CDO)** ผู้บริหารรักษาความปลอดภัยระดับสูง **(Chief Security Officer** หรือ **CSO)** และบริกรข้อมูล **(Data Steward)** ซึ่งเป็นผู้ที่มีหน้าที่แก้ไขและปรับปรุงข้อมูล จนถึง เจ้าของข้อมูล **(Data owner)** เป็นต้น ดังนั้นมีจำเป็นอย่างยิ่งที่หน่วยงานที่รับผิดชอบฐานข้อมูลด้านความมั่นคงจะต้องปรับเปลี่ยนโครงสร้างบุคลากรให้มีผู้รับผิดชอบโดยตรงเพื่อทำหน้าที่ต่างๆที่เกี่ยวเข้องกับการกำกับดูแลข้อมูลให้เป็นไปตามมาตรฐานการธรรมาภิบาลข้อมูลของชาติและของนานาชาติ



แผนภาพที่ ๒๑ ตัวอย่างโครงสร้างบุคคลากรกำกับดูแลข้อมูลของหน่วยงาน
ที่มา: เอกสาร กรอบการกำกับดูแลข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)



แผนภาพที่ ๒๒ ตัวอย่างกระบวนการกำกับดูแลข้อมูลของหน่วยงาน
ที่มา: เอกสาร กรอบการกำกับดูแลข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๔.๓ สรุป กิจกรรม ผลลัพธ์ และงบประมาณของโครงการ

โครงการพัฒนาระบบแพลตฟอร์มระดับองค์กร (Enterprise Big Data Platform) ระยะที่ ๒ ในปีที่ ๒ ใช้ระยะเวลาดำเนินการ ๑๒ เดือน สามารถแยกกิจกรรมออกเป็นส่วนๆ พร้อมผลลัพธ์ที่ได้จากกิจกรรม และงบประมาณที่ใช้ในโครงการ ดังนี้

กิจกรรม	ผลลัพธ์	งบประมาณ (ล้านบาท)
๑. กำหนดนโยบายข้อมูลและมาตรฐานการกำกับดูแลข้อมูลด้านความมั่นคง	นโยบายข้อมูลและมาตรฐานการปฏิบัติงานด้านการกำกับดูแลข้อมูลด้านความมั่นคง	๕
๒. พัฒนาระบบ Enterprise Big data platform (on-premise platform)	ระบบ Enterprise Big Data platform	๑๐
๓. พัฒนาระบบบิ๊กดาต้าแพลตฟอร์มสำรอง Big data DR-site (on-cloud platform)	ระบบ Big data DR-Site	๑๐
๔. พัฒนาระบบ Backup and Disaster	ระบบ Backup and Disaster Recovery	๕

Recovery (BDR)	(BDR)	
๕. พัฒนาระบบ data service and sharing	ระบบบริการและแลกเปลี่ยนข้อมูล	๕
๕. พัฒนาระบบ Digital Transformation	ระบบเทคโนโลยีสาระสนเทศเพื่อการปฏิรูปองค์กรให้เป็นดิจิทัลจำนวน ๓ ระบบ	๑๐
๖. พัฒนาระบบธรรมาภิบาลข้อมูล	ระบบธรรมาภิบาลข้อมูล	๑๐
๗. พัฒนาระบบ Master Data Management	ระบบการบริหารจัดการข้อมูลหลักด้านความมั่นคง (National Security Master Data Management)	๑๐
๘. พัฒนาระบบวิเคราะห์และทำรายงานขั้นสูง	ระบบวิเคราะห์และรายงาน ด้านความมั่นคง จำนวน ๓ โจทย์ โดยใช้เทคนิค Data analytics and visualization ขั้นสูง	๑๕
๙. การฝึกอบรมบุคลากรบิ๊กดาต้าขั้นสูง (Advanced big data training)	หลักสูตร big data admin ขั้นสูง หลักสูตร data engineer ขั้นสูง หลักสูตร data analytics ขั้นสูง หลักสูตร data visualization ขั้นสูง หลักสูตรบิ๊กดาต้าสำหรับผู้บริหารขั้นสูง	๑๕
รวมทั้งสิ้น		๙๕

บทที่ ๕ การพัฒนาบิ๊กดาต้าด้านความมั่นคงระยะที่ ๓ ปีที่ ๓

โครงการระยะที่ ๓ จะเป็นการพัฒนาในส่วนของการบูรณาการข้อมูลร่วมกับหน่วยงานอื่น ทั้งภาครัฐและเอกชน ที่มีส่วนเกี่ยวข้องกับงานความมั่นคง โดยจะทำการเชื่อมต่อระบบฐานข้อมูลบิ๊กดาต้า เข้ากับหน่วยงานดังกล่าว ผ่านระบบบริหารจัดการส่วนกลาง หรือแพลตฟอร์มการบูรณาการเชื่อมโยงข้อมูลแบบสมบูรณ์ (Fully-integrated Big Data Platform) ทำให้สามารถดำเนินการประสานงานได้อย่างมีประสิทธิภาพและรวดเร็วมากยิ่งขึ้น นอกจากนี้ระบบการนำเข้าข้อมูล แบบ real-time จะถูกพัฒนาให้มีประสิทธิภาพมากยิ่งขึ้น โดยระบบบิ๊กดาต้าแพลตฟอร์ม สามารถรองรับการส่งข้อมูลจากอุปกรณ์ IoT เช่น sensor แบบ real-time ได้

๕.๑ วัตถุประสงค์ของโครงการ

๕.๑.๑ เพื่อพัฒนาระบบการเชื่อมโยงข้อมูลบิ๊กดาต้า ของสำนักงานสภาความมั่นคงแห่งชาติให้มีศักยภาพมากยิ่งขึ้น โดยสามารถนำข้อมูลหรือการดำเนินการต่างๆ เกี่ยวกับข้อมูล มาบูรณาการร่วมกับหน่วยงานอื่นทั้งภาครัฐและเอกชนที่มีบทบาทการทำงานร่วมกัน

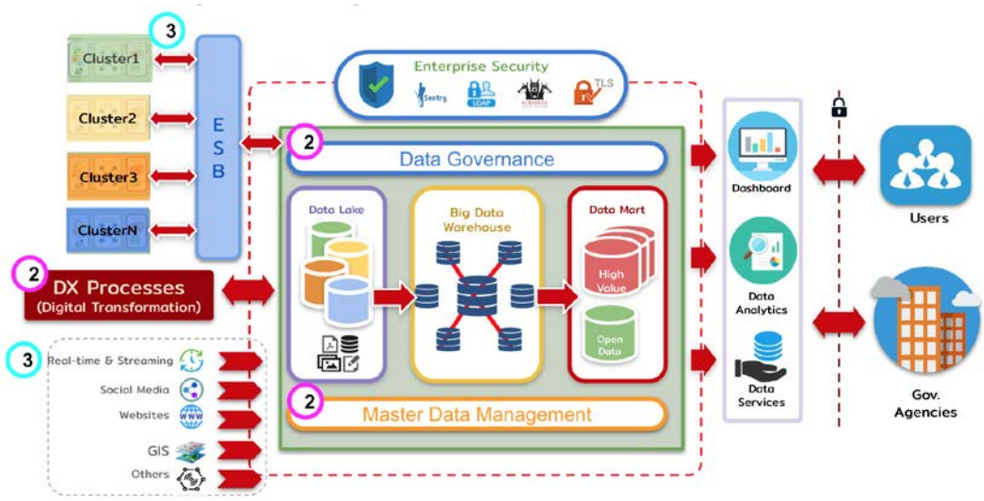
๕.๑.๒ เพื่อเพิ่มสักยภาพในการประมวลผลต่อข้อมูลแบบ real-time ให้รองรับข้อมูลที่ถูกส่งมาจากอุปกรณ์ IoT (Internet of Things) และ censor ต่างๆ ได้ เพื่อสนับสนุนเรื่องการเฝ้าระวังภัยคุกคามต่างๆได้ดียิ่งขึ้น

๕.๑.๓ เพื่อพัฒนาระบบบิ๊กดาต้า ให้สามารถประยุกต์ใช้ ระบบการประมวลผลที่มีปัญญาประดิษฐ์ (Artificial Intelligence) เข้ามาช่วยเหลือในการทำงานของบุคลากร เพื่อลดระยะเวลาทำงานของบุคลากร

๕.๒ รายละเอียดการพัฒนาระบบตามแผนการดำเนินการในระยะที่ ๓ ปีที่ ๓

๕.๒.๑ โครงการพัฒนาระบบแพลตฟอร์มการเชื่อมโยงข้อมูลแบบสมบูรณ์ (Fully-integrated Big Data Platform)

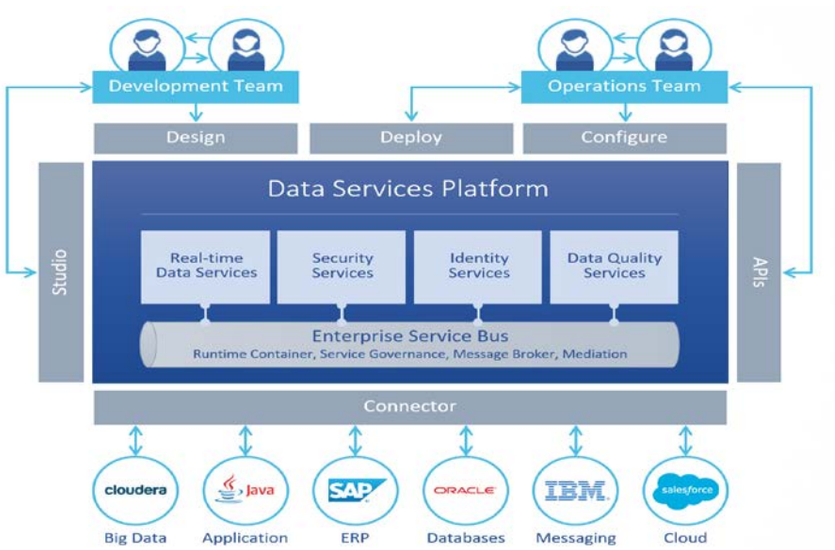
ระบบบิ๊กดาต้าที่ได้รับการพัฒนามาจาก ๒ ระยะแรก จะมีความพร้อมในการประสานงานด้านการกระจายข้อมูลร่วมกับ ระบบ ฐานข้อมูล บิ๊กดาต้าขององค์กรอื่น ๆ ในส่วนของการเชื่อมต่อระบบนั้นจะทำงานผ่านระบบบริการ รับ-ส่ง ข้อมูลระดับองค์กร (Enterprise Service Bus) หรือ ESB ที่รองรับการทำงานการบริหารจัดการข้อมูลและบูรณาการข้อมูลระดับสูง ในรูปแบบ multi-portal gateway application ทำให้การเข้าถึงข้อมูลหรือการกระจายข้อมูลไปสู่หน่วยงานภายนอกมีความรวดเร็วและมีประสิทธิภาพมาก



แผนภาพที่ ๒๓ แสดงสถาปัตยกรรม Fully-integrated Big Data Platform ระยะที่ ๓ ปีที่ ๓

๕.๒.๒ Enterprise Data service and sharing using ESB

ข้อมูลที่มากมายมหาศาลที่ถูกถ่ายโอนผ่านไปมา บนระบบบิ๊กดาต้าจากองค์กรสู่องค์กร ทั้งภายในและภายนอกหน่วยงานของสำนักงานสภาความมั่นคงแห่งชาตินั้น จำเป็นต้องมีระบบบริหารจัดการที่มีประสิทธิภาพสูง คือ Enterprise Service Bus (ESB) ซึ่งประกอบไปด้วย messaging, web services, data services, sercurity management เป็นต้น โดยองค์ประกอบเหล่านี้จะช่วยส่งเสริมให้ผู้ใช้สามารถเข้าถึงข้อมูลเพื่อดำเนินการต่อข้อมูลเหล่านั้นได้ผ่านอุปกรณ์ที่หลากหลายและมีความปลอดภัยในการรักษาความลับของข้อมูล เช่น การกำหนดสิทธิ์ในการเข้าถึงข้อมูลชั้นความลับต่างๆ เพื่อเพิ่มประสิทธิภาพในการทำงานของเจ้าหน้าที่ได้มากยิ่งขึ้น



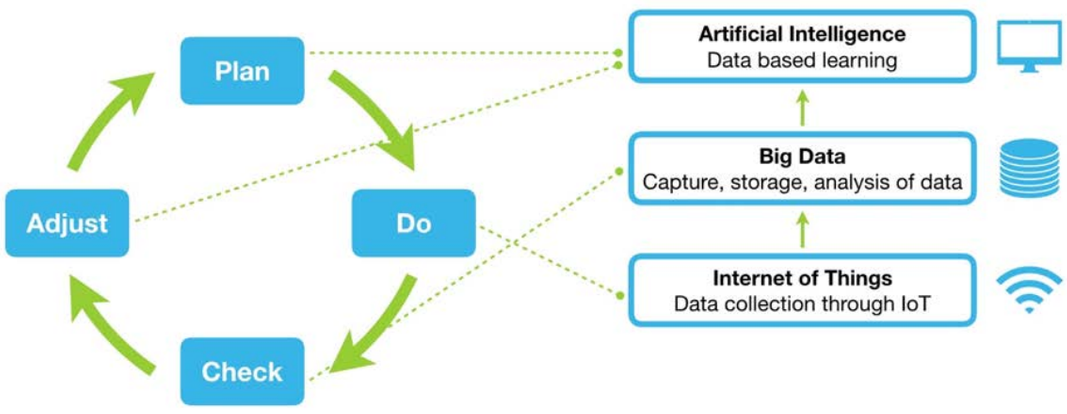
แผนภาพที่ ๒๔ แผนภาพโครงสร้างระบบ Enterprise Service Bus (ESB)

๕.๒.๓ Enterprise Data Governance for High Reliability & Availability Data Interchange

ยกระดับความเป็นเอกสิทธิ์ในการถือครองข้อมูลของหน่วยงานภายใน จาก **Data Governance** ที่เป็นนโยบายเฉพาะภายในหน่วยงานไปสู่ระดับ **Enterprise Data Governance** ซึ่งเป็นการดำเนินการที่ทำให้ข้อมูลที่ครอบครองอย่างถูกต้องตามกฎหมาย อยู่ในมาตรฐานที่ตรงกับหน่วยงานภายนอกในทุกด้าน เช่น การรักษาความปลอดภัย การกำหนดมาตรฐานข้อมูล การกำหนดกรรมวิธีทางข้อมูล เป็นต้น ทั้งนี้เพื่อทำให้การประสานงานในการแลกเปลี่ยนข้อมูลรวดเร็ว ถูกต้อง มีรูปแบบเดียวกัน และปลอดภัยต่อการโจรกรรม

๕.๒.๔ Data integration for unstructured and real-time data

นอกจากนี้ระบบแพลตฟอร์มการเชื่อมโยงข้อมูลแบบสมบูรณ์ (Fully-integrated Big Data Platform) ยังมีการพัฒนาการนำเข้าข้อมูลแบบ Real-time ให้รองรับการส่งข้อมูลอย่างต่อเนื่องจากระบบของอุปกรณ์ IoT ที่มีประโยชน์ต่อการปฏิบัติงานด้านความมั่นคง ให้สามารถเพิ่มการปฏิบัติงานได้หลายมิติ เช่น อุปกรณ์ส่งสัญญาณติดตามตัวหรือ Sensor ต่างๆ สามารถแจ้งเตือนเข้ามาที่ระบบ บิ๊กดาต้าได้ตลอดเวลา และในส่วนของระบบฐานข้อมูลนั้น จะสามารถรายงานการติดตามแจ้งเตือนและประมวลผลวิเคราะห์ถึงภัยคุกคามได้ทันที สำหรับตัวแพลตฟอร์มจะยังคงเป็น Enterprise big data platform ตามที่ได้พัฒนาในปีที่ผ่านมาเหมือนเดิม โดยในส่วนการวิเคราะห์ข้อมูลจะมีการนำ AI และ Machine Learning ระดับสูงที่สามารถเรียนรู้การวิเคราะห์ข้อมูลเชิงลึกหรือ Deep Learning เข้ามาใช้เพื่อให้ผลการวิเคราะห์แม่นยำมากยิ่งขึ้น สำหรับการพัฒนาบุคลากรจะเริ่มมีหลักสูตรอบรมด้านนักวิทยาศาสตร์ข้อมูล (Data scientist) เพิ่มเข้ามาจากหลักสูตรเดิม



แผนภาพที่ ๒๕ แผนภาพการทำงานโดยรวมของระบบ Real-timer IoT Data

๕.๓ สรุป กิจกรรม ผลลัพธ์ และงบประมาณของโครงการ

โครงการพัฒนาระบบแพลตฟอร์มการเชื่อมโยงข้อมูลแบบสมบูรณ์ (Fully-integrated Big Data Platform) ระยะที่ ๓ ปีที่ ๓ ใช้ระยะเวลาดำเนินการ ๑๒ เดือน สามารถแยกกิจกรรมออกเป็นส่วนๆ พร้อมผลลัพธ์ที่ได้จากกิจกรรม และงบประมาณที่ใช้ในโครงการ ดังนี้

กิจกรรม	**ผลลัพธ์**	**งบประมาณ (ล้านบาท)**
๑. กำหนดมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน	มาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน	๕
๒. พัฒนาระบบ Fully-integrated Big Data Platform	ระบบ Fully-integrated Big Data Platform	๑๕
๓. พัฒนาระบบแลกเปลี่ยนข้อมูลแบบ Enterprise Service Bus (ESB)	ระบบแลกเปลี่ยนข้อมูลแบบ ESB	๑๕
๔. พัฒนาระบบ IoT platform	ระบบ IoT platform	๑๕
๕. พัฒนาระบบนำเข้าและจัดเก็บข้อมูลแบบ Real-time	ระบบนำเข้าและจัดเก็บข้อมูลแบบ real-time	๑๕
๖. พัฒนาระบบวิเคราะห์ด้วย AI และ Machine Learning	ระบบวิเคราะห์ข้อมูลด้วย AI และ Machine Learning	๑๕
๗. การฝึกอบรมนักวิทยาศาสตร์ข้อมูล	หลักสูตร Master data management หลักสูตร ESB data exchange หลักสูตร IoT management หลักสูตร Real-time streaming หลักสูตร AI & Machine Learning หลักสูตร Data science	๑๕
รวมทั้งสิ้น		๙๕

บทที่ ๖ การพัฒนาบิ๊กดาต้าด้านความมั่นคงระยะที่ ๔ ปีที่ ๔

โครงการในปีสุดท้ายจะเป็นการพัฒนาต่อจากระบบในห้วงที่ผ่านมา ทั้งในส่วนของระบบบิ๊กดาต้าและระบบความปลอดภัยระดับองค์กร ระบบบริหารจัดการข้อมูลระดับองค์กร สำหรับในส่วนระบบวิเคราะห์ข้อมูลในปีนี้จะยกระดับ ให้มีการใช้เทคโนโลยี AI และ Machine learning มาใช้ทำระบบอัจฉริยะ ที่เรียกว่า Data intelligence

๖.๑ วัตถุประสงค์โครงการ

๖.๑.๑ เพื่อพัฒนาระบบปัญญาประดิษฐ์ (AI) จากโครงการระยะที่ ๓ ให้มีความชาญฉลาดมากยิ่งขึ้น โดยระบบจะทำการวิเคราะห์รูปแบบของข้อมูล (Pattern) ในเชิงสถิติ เพื่อหาผลลัพธ์ขั้นต้นออกมา เป็นคำแนะนำสำหรับการทำแผนงานในอนาคต

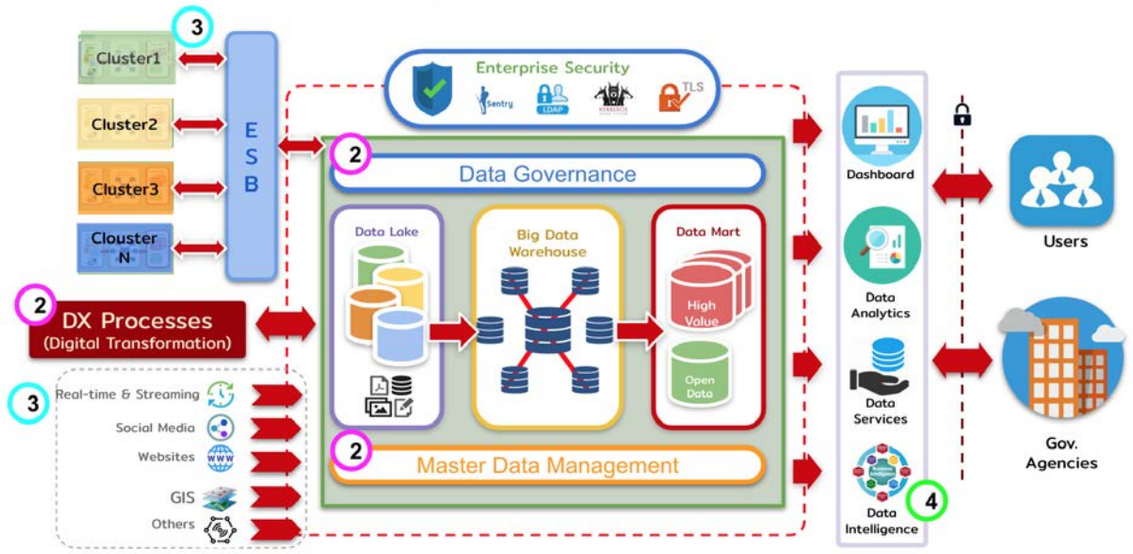
๖.๑.๒ เพื่อให้มีทรัพยากรในการอบรมบุคลากร ให้มีขีดความสามารถด้านนักวิทยาศาสตร์ข้อมูล (Data scientist) ซึ่งจะทำงานร่วมกับระบบ AI

๖.๑.๓ เพื่อเพิ่มสักยภาพของระบบเฝ้าระวังภัยคุกคามต่างๆ ให้มีความฉลาดมากยิ่งขึ้น ด้วยระบบ AI ที่เข้ามาควบคุมการทำงานเชิงลึก

๖.๒ รายละเอียดการพัฒนาระบบตามแผนการดำเนินการในระยะที่ ๔ ปีที่ ๔

๖.๒.๑ โครงการพัฒนาระบบระบบข้อมูลความมั่นคงอัจฉริยะ (National Security Data Intelligence)

เป็นระบบที่เน้นการนำเอาเทคโนโลยี AI และ Machine learning มาทำการวิเคราะห์ ด้วยโมเดลที่สามารถเรียนรู้ได้ด้วยตนเอง โดยจะทำให้ระบบมีการปรับตัวได้เองอัตโนมัติ หรือเป็นระบบแบบอัจฉริยะ ซึ่งข้อมูลที่จะนำมาใช้จะมาจากระบบข้อมูลที่รอบด้าน ทั้งข้อมูลจากฐานข้อมูลปัจจุบันและข้อมูลจากระบบ IoT ที่เป็นแบบ real-time นอกจากนี้จะเน้นการพัฒนาโจทย์ที่เป็นระบบอัจฉริยะกับงานด้านความมั่นคงจำนวน ๔ ด้าน (โจทย์ละหนึ่งด้าน) และมีการฝึกอบรมนักวิทยาศาสตร์ข้อมูลขั้นสูงในโครงการควบคู่ไปด้วย



แผนภาพที่ ๒๖ แสดงสถาปัตยกรรม National Security Data Intelligence ระยะที่ ๔ ปีที่ ๔

๖.๒.๒ AI and Machine Learning

AI หรือ Artificial Intelligence กล่าวโดยสรุป คือ ระบบที่สร้างขึ้นที่มีความสามารถปฏิบัติภารกิจที่ได้โดยปราศจากการควบคุมจากมนุษย์ และมีพฤติกรรมหรือการทำงานคล้ายมนุษย์ โดยตัดสินใจขึ้นอยู่กับสถานการณ์ (input factors) เทียบกับประสบการณ์ที่ผ่านมา (learning data) และสามารถนำผลลัพธ์จากการปฏิบัติงานมาปรับปรุงการปฏิบัติงานครั้งต่อไป (re-learning) เพื่อให้การปฏิบัติภารกิจมีประสิทธิ์ที่ภาพสูงสุด

Machine Learning เป็นส่วนย่อยของระบบ AI เป็นกระบวนการทางการเขียนโปรแกรมคอมพิวเตอร์เพื่อใช้กลุ่มข้อมูลในการประมวลหาโมเดล (Model) หรือฟังก์ชันทางคณิตศาสตร์ โดยผลลัพธ์ของโมเดลที่ได้เปรียบเหมือนสมองของระบบ AI ใช้ในการตัดสินใจในการปฏิบัติ (Actions) จากสถานการณ์ (input factors) ไม่ว่าจะเคยมีหรือไม่มีอยู่ในกลุ่มข้อมูลก็ตาม

ในด้านแพลตฟอร์มส่วนที่สนับสนุน AI และ Machine Learning ประกอบด้วย ส่วนของการบริการ (Services) สำหรับนักวิทยาศาสตร์ข้อมูล (Data Scientist) ใช้ในการเขียนโปรแกรมเพื่อการทำ Machine Learning สร้างโมเดล ได้แก่ Python และ Rstudio ส่วนบริการที่ใช้ในการฝึกและทดสอบโมเดล ได้แก่ Tensorflow และส่วนบริการในการเรียกใช้โมเดล (deploy) กับระบบ ได้แก่ API Service ซึ่งส่วนบริการเหล่านี้จำเป็นจะต้องทำงานร่วมกันเพื่อดำเนินการกระบวนงานของ Machine Learning ตั้งแต่ เตรียมข้อมูล (Preprocess data หรือ Prepare data), สร้างโมเดล (Create model), ฝึกโมเดล (Train model), ประเมินผลโมเดล (Evaluate model), เรียกใช้โมเดล (Deploy model) และ การปรับปรุงโมเดลจากข้อมูลใหม่ (Re-train model) เพื่อให้ได้โมเดลหรือสมองของระบบที่ประสิทธิภาพ

๖.๒.๓ Data Intelligence

Data Intelligence คือระบบ AI ที่สนับสนุนการดำเนินการปฏิบัติภารกิจโดยใช้การตัดสินใจอย่างชาญฉลาด (Intelligence) จากข้อมูล (Data) ที่มี โดยการประสานการทำงานในส่วนต่าง ๆ ของแพลตฟอร์มตั้งแต่ ฐานข้อมูล ระบบเชื่อมโยงข้อมูล ระบบวิเคราะห์ข้อมูล รวมถึง AI และ Machine Learning เพื่อประยุกต์ใช้ AI เป็นศูนย์กลางในการประมวลข้อมูล แจ้งเตือน และตัดสินใจกำหนดวางแผนการปฏิบัติงานต่างๆ และในด้านการรักษาความปลอดภัย สามารถประยุกต์ใช้ระบบ Data Intelligence ในการดำเนินการต่างๆ ได้ ดังนี้

๖.๒.๓.๑ การปฏิบัติการด้านข้อมูล (Information Operations)

การดำเนินการในด้านการประมวลข้อมูลต่างๆ เช่น การค้นหาข้อมูลเชิงลึก (Insigns) การค้นหาความเชื่อมโยงของข้อมูล การตรวจสอบยืนยันความถูกต้องของข้อมูล หรือ การตรวจหาความผิดปกติ (Anomolies) เป็นต้น

๖.๒.๓.๒ การสั่งการและควบคุม (Command and Control)

เป็นการดำเนินการประมวลและวิเคราะห์ข้อมูลต่างๆ ที่เกี่ยวข้อง ซึ่งเป็นการประมวลข้อมูลรอบด้านในทุกมิติ เพื่อนำผลวิเคราะห์มาช่วยในการวางแผน ดำเนินการ ติดตามสถานการณ์รวมถึงประเมินสถานการณ์ คาดการณ์แนวโน้ม เพื่อช่วยให้การปฏิบัติภารกิจดำเนินไปอย่างมีประสิทธิภาพ

๖.๒.๓.๓ ระบบการเฝ้าระวังภัย (Surveillance System)

ระบบช่วยในการเฝ้าติดตาม และวิเคราะห์ข้อมูลทางด้านต่างๆ เพื่อตรวจหาสิ่งผิดปกติ และเมื่อตรวจพบสิ่งผิดปกติ ระบบจะสามารถแจ้งเตือนผู้ที่รับผิดชอบ รวมทั้งประสานข้อมูลผู้ที่เกี่ยวข้อง และการให้แนะนำการปฏิบัติ เพื่อให้ดำเนินการเป็นไปด้วยความรวดเร็วมีประสิทธิภาพ

๖.๒.๓.๔ ระบบการตรวจพบค้นหา (Detection System)

ระบบช่วยในการตรวจหาบุคคล หรือวัตถุต้องสงสัย เช่น ทะเบียนรถ หรือบุคคลเป้าหมาย จากการประยุกต์ใช้ Image processing ร่วมกับฐานข้อมูลบุคคลและวัตถุต้องสงสัย เพื่อค้นหา เฝ้าระวัง และตรวจจับได้อย่างมีประสิทธิภาพมากขึ้น ลดความเสี่ยงภัยให้กับเจ้าหน้าที่ปฏิบัติงาน พร้อมทั้งเพิ่มประสิทธิภาพในการปฏิบัติหน้าที่

๖.๓ สรุป กิจกรรม ผลลัพธ์ และงบประมาณของโครงการ

โครงการพัฒนาระบบ National Security Data Intelligence ระยะที่ ๔ ในปีที่ ๔ ใช้ระยะเวลาดำเนินการ ๑๒ เดือน สามารถแยกกิจกรรมออกเป็นส่วนๆ พร้อมผลลัพธ์ที่ได้จากกิจกรรม และงบประมาณที่ใช้ในโครงการ ดังนี้

กิจกรรม	**ผลลัพธ์**	**งบประมาณ (ล้านบาท)**
๑. กำหนดมาตรฐานการให้บริการข้อมูลอัจฉริยะ	มาตรฐานการให้บริการข้อมูลอัจฉริยะ	๕
๒. พัฒนาระบบ National Security Data Intelligence	ระบบ National Security Data Intelligence	๒๐
๓. พัฒนาระบบ IoT platform ขั้นสูง	ระบบ IoT platform ขั้นสูง	๑๕
๔. พัฒนาระบบวิเคราะห์ด้วย AI และ Machine Learning ขั้นสูง	ระบบวิเคราะห์ด้วย AI และ Machine Learning ขั้นสูง	๑๕
๕. พัฒนาระบบอัจฉริยะด้านความมั่นคง จำนวน ๔ โจทย์	ระบบอัจฉริยะด้านความมั่นคง จำนวน ๔ โจทย์	๒๕
๖. การฝึกอบรมนักวิทยาศาสตร์ข้อมูลขั้นสูง	หลักสูตร IoT management ขั้นสูง หลักสูตร Real-time streaming ขั้นสูง หลักสูตร AI & Machine Learning ขั้นสูง หลักสูตร Data intelligence	๑๕
รวมทั้งสิ้น		**๙๕**

ผนวก ก
รายการคุณลักษณะเฉพาะของระบบบิ๊กดาต้าแพลตฟอร์ม

๑. เครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบบิ๊กดาต้าแพลตฟอร์ม (Big data platform) ประกอบด้วย

๑.๑ เครื่องแม่ข่ายหลัก (Master node) จำนวน ๓ เครื่อง (โหนด) เพื่อทำหน้าที่เป็นส่วนควบคุมการทำงานของบริการต่างๆ โดยแต่ละโหนด มีคุณลักษณะดังนี้

๑.๑.๑ มีหน่วยประมวลผลกลางชนิด Intel XEON หรือดีกว่า โดยมีจำนวน Core ไม่น้อยกว่า ๑๖ Core มีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า ๒.๑ GHz

๑.๑.๒ มีหน่วยความจำหลักรวมขนาดไม่น้อยกว่า ๒๕๖ GB แบบ DDR๔ RDIMM หรือดีกว่า และรองรับการทำงานแบบ Advance ECC ได้

๑.๑.๓ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SSD หรือดีกว่า ทำเป็น RAID ๑ สำหรับระบบปฏิบัติการ ความจุไม่น้อยกว่า ๑ TB จำนวน ๒ หน่วย (๑ TB x ๒)

๑.๑.๔ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SAS หรือดีกว่า ทำเป็น JBOD สำหรับ HDFS ขนาดไม่น้อยกว่า ๒ TB จำนวน ๔ หน่วย (๒ TB x ๔) หรือความจุรวม ๘ TB เป็นอย่างน้อย

๑.๑.๕ มีหน่วยควบคุมการจัดเก็บข้อมูล (Controller) แบบ SATA หรือดีกว่าซึ่งสนับสนุนการทำ RAID ๐,๑,๕,๖ และ ๑๐ ได้เป็นอย่างน้อย

๑.๑.๖ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑๐ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๑.๗ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๒ เครื่องแม่ข่ายสำหรับจัดเก็บและประมวลผลข้อมูล Data node จำนวน ๕ เครื่อง (โหนด) และมีหน่วยเก็บข้อมูลทุกโหนดรวมกันจำนวนรวมอย่างน้อย ๑๐๐ TB เพื่อทำหน้าที่เป็นส่วนจัดเก็บข้อมูล HDFS และประมวลผลข้อมูลแบบขนาน (Parallel computing) ในระบบบิ๊กดาต้า โดยแต่ละโหนด มีคุณลักษณะดังนี้

๑.๒.๑ มีหน่วยประมวลผลกลางชนิด Intel XEON หรือดีกว่า โดยมีจำนวน Core ไม่น้อยกว่า ๒๐ Core มีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า ๒.๑ GHz

๑.๒.๒ มีหน่วยความจำหลักรวมขนาดไม่น้อยกว่า ๒๕๖ GB แบบ DDR4 RDIMM หรือดีกว่า และรองรับการทำงานแบบ Advance ECC ได้

๑.๒.๓ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SSD หรือดีกว่า ทำเป็น RAID ๑ สำหรับระบบปฏิบัติการ ความจุไม่น้อยกว่า ๑ TB จำนวน ๒ หน่วย (๑ TB x ๒)

๑.๒.๔ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SAS หรือดีกว่า ทำเป็น JBOD สำหรับ HDFS ขนาดไม่น้อยกว่า ๔TB จำนวน ๕ หน่วย (๔ TB x ๕) หรือความจุรวม ๒๐ TB เป็นอย่างน้อย

๑.๒.๕ มีหน่วยควบคุมการจัดเก็บข้อมูล (Controller) แบบ SATA หรือดีกว่า ซึ่งสนับสนุนการทำ RAID ๐,๑,๕,๖ และ ๑๐ ได้เป็นอย่างน้อย

๑.๒.๖ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑๐ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๒.๗ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๓ เครื่องแม่ข่ายสำหรับ Active Directory (AD) server จำนวน ๑ เครื่อง มีคุณลักษณะดังนี้

๑.๓.๑ มีหน่วยประมวลผลกลางชนิด Intel XEON หรือดีกว่า โดยมีจำนวน Core ไม่น้อยกว่า ๔ Core มีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า ๒.๑ GHz

๑.๓.๒ มีหน่วยความจำหลักรวมขนาดไม่น้อยกว่า ๓๒ GB แบบ DDR 4 RDIMM หรือดีกว่า และรองรับการทำงานแบบ Advance ECC ได้

๑.๓.๓ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SSD หรือดีกว่า ทำเป็น RAID ๑ สำหรับระบบปฏิบัติการ ความจุไม่น้อยกว่า ๑ TB จำนวน ๒ หน่วย (๒ TB x ๒)

๑.๓.๔ มีหน่วยควบคุมการจัดเก็บข้อมูล (Controller) แบบ SATA หรือดีกว่า ซึ่งสนับสนุนการทำ RAID ๐,๑,๕,๖ และ ๑๐ ได้เป็นอย่างน้อย

๑.๓.๕ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑๐ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๓.๖ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๓.๗ มีลิขสิทธิ์ระบบปฏิบัติการ Windows version 2016 เป็นอย่างน้อย

๑.๔ เครื่องแม่ข่ายสำหรับ ETL server จำนวน ๒ เครื่อง แต่ละเครื่องมีคุณลักษณะดังนี้

๑.๔.๑ มีหน่วยประมวลผลกลางชนิด Intel XEON หรือดีกว่า โดยมีจำนวน Core ไม่น้อยกว่า ๘ Core มีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า ๒.๑ GHz

๑.๔.๒ มีหน่วยความจำหลักรวมขนาดไม่น้อยกว่า ๑๒๘ GB แบบ DDR ๔ RDIMM หรือดีกว่า และรองรับการทำงานแบบ Advance ECC ได้

๑.๔.๓ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SSD หรือดีกว่า ทำเป็น RAID ๑ สำหรับระบบปฏิบัติการ ความจุไม่น้อยกว่า ๒ TB จำนวน ๒ หน่วย (๒ TB x ๒)

๑.๔.๔ มีหน่วยควบคุมการจัดเก็บข้อมูล (Controller) แบบ SATA หรือดีกว่า ซึ่งสนับสนุนการทำ RAID ๐,๑,๕,๖ และ ๑๐ ได้เป็นอย่างน้อย

๑.๔.๕ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑๐ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๔.๖ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๔.๗ มีลิขสิทธิ์ระบบปฏิบัติการ Windows version 2016 เป็นอย่างน้อย

๑.๕ เครื่องแม่ข่ายสำหรับ BI server จำนวน ๑ เครื่อง มีคุณลักษณะดังนี้

๑.๕.๑ มีหน่วยประมวลผลกลางชนิด Intel XEON หรือดีกว่า โดยมีจำนวน Core ไม่น้อยกว่า ๘ Core มีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า ๒.๑ GHz

๑.๕.๒ มีหน่วยความจำหลักรวมขนาดไม่น้อยกว่า ๖๔ GB แบบ DDR ๔ RDIMM หรือดีกว่า และรองรับการทำงานแบบ Advance ECC ได้

๑.๕.๓ มีหน่วยเก็บข้อมูล Hard Disk Drive ชนิด SSD หรือดีกว่า ทำเป็น RAID ๑ สำหรับระบบปฏิบัติการ ความจุ ๒ TB จำนวน ๒ หน่วย (๒ TB x ๒)

๑.๕.๔ มีหน่วยควบคุมการจัดเก็บข้อมูล (Controller) แบบ SATA หรือดีกว่า ซึ่งสนับสนุนการทำ RAID ๐,๑,๕,๖ และ ๑๐ ได้เป็นอย่างน้อย

๑.๕.๕ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑๐ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๕.๖ มีอุปกรณ์เชื่อมต่อ Ethernet แบบ ๑ Gbps จำนวน ๒ พอร์ต เป็นอย่างน้อย

๑.๕.๗ มีลิขสิทธิ์ระบบปฏิบัติการ Windows version 2016 เป็นอย่างน้อย

๒. อุปกรณ์ Networking Switch จำนวน ๑ ระบบ มีคุณลักษณะดังนี้

๒.๑ อุปกรณ์ Networking Switch สำหรับเชื่อมต่อระหว่างเครื่องแม่ข่าย (Server Switch) ภายในระบบบิ๊กดาต้า จำนวน ๒ เครื่อง โดยมีคุณสมบัติอย่างน้อย ดังนี้

๒.๑.๑ มีช่องเชื่อมต่อระบบเครือข่าย แบบ ๑/๑๐ Gb Base-T จำนวนไม่น้อยกว่า ๒๔ ช่อง

๒.๑.๒ รองรับการเชื่อมต่อระบบเครือข่ายแบบ ๑๐ Gb SFP+ จำนวนไม่น้อยกว่า ๔ ช่อง

๒.๑.๓ รองรับการเชื่อมต่อระบบเครือข่ายแบบ ๔๐ Gb QFP+ จำนวนไม่น้อยกว่า ๒ ช่อง

๒.๑.๔ มีขนาดของ Switching capacity ไม่น้อยกว่า ๙๖๐ Gbps

๒.๒ อุปกรณ์ Networking switch สำหรับเครื่องแม่ข่าย (Management Switch) จำนวน ๑ เครื่อง มีคุณสมบัติอย่างน้อย ดังนี้

๒.๒.๑ มีช่องต่อสัญญาณ (พอร์ต) แบบ ๑๐/๑๐๐/๑๐๐๐ BASE-T จำนวนไม่น้อยกว่า ๒๔ พอร์ต

๒.๒.๒ มีช่องต่อสัญญาณ (พอร์ต) แบบ 1 GE จำนวนไม่น้อยกว่า ๔ พอร์ต

๒.๒.๓ อุปกรณ์ต้องมีขนาดของ Forwarding Bandwidth ไม่น้อยกว่า ๑๐๘ Gbps

๒.๒.๔ สนับสนุนการทำงาน Virtual LAN (VLANs) ตามมาตรฐาน IEEE 802.1Q ได้

๒.๒.๕ สนับสนุนการทำ Private VLAN และ Private VLAN Edge ได้

๒.๒.๖ มีพอร์ต Console แบบ USB และ/หรือ RJ-45 Console

๓. อุปกรณ์จัดเก็บข้อมูลแบบ SAN (Storage Area Network) จำนวน ๑ ระบบ สำหรับการสำรอง และ กู้คืนข้อมูล (Backup and recovery) ในระบบบิ๊กดาต้าแพลตฟอร์ม ดังนี้

๓.๑ เป็นอุปกรณ์ ระบบจัดเก็บข้อมูลแบบ Network Storage เพื่อให้บริการจัดเก็บข้อมูลแบบ unstructured data ผ่านระบบเครือข่ายความเร็วสูง

๓.๒ มีหน้าจอการใช้งานแบบ Web browser UI หรือ GUI เพื่อให้สามารถใช้งานง่าย

๓.๓ มีหน่วยประมวลผลกลางชนิด Intel XEON หรือดีกว่า โดยมีจำนวน Core ไม่น้อยกว่า ๘ Core มีความเร็วสัญญาณนาฬิกาไม่ต่ำกว่า ๒.๑ GHz

๓.๔ หน่วยความจำแต่ละ Controller อย่างน้อย ๓๒ GB

๓.๕ หน่วยความจำ storage แบบ HDD ความจุรวมไม่น้อยกว่า ๕๐ TB

๓.๖ สามารถทำการบีบอัดข้อมูลที่จัดเก็บใน storage ได้

๓.๗ อุปกรณ์ต้องสามารถติดตั้งอยู่ในโครงตู้ (chassis) ความสูงไม่เกิน 42U ได้

๔. ซอฟต์แวร์บริหารจัดการระบบบิ๊กดาต้า โดยพัฒนามาจากสถาปัตยกรรมของ Apache Hadoop Open Source และมีคุณสมบัติอย่างน้อยดังนี้

๔.๑ ระบบบริหารจัดการไฟล์แบบ HDFS (Hadoop filesystem) ซึ่งเป็นระบบไฟล์แบบกระจาย (Distributed filesystem) ของ Hadoop

๔.๒ สามารถจัดเก็บข้อมูลได้ทั้งข้อมูลชนิดโครงสร้าง (Structured data) ข้อมูลกึ่งโครงสร้าง (Semi-Structured data) และข้อมูลแบบไม่มีโครงสร้าง (Unstructured data) จัดเก็บข้อมูลในรูปแบบมาตรฐานของ Hadoop File System ที่รองรับการจัดเก็บข้อมูลใน Hive/Impala (SQL-lke database) และ HBase (NoSQL database) ได้เป็นอย่างน้อย

๔.๓ สามารถสืบค้นข้อมูลด้วยภาษา HQL (Hive Query Language) ผ่านบริการของ Hive และ Impala และรองรับการระบุเงื่อนไขการดึงข้อมูลเป็นภาษาไทยได้เป็นอย่างน้อย

๔.๔ สนับสนุนการประมวลผลข้อมูลแบบขนาน (Parallel computing) โดยใช้ MapReduce ได้เป็นอย่างน้อย

๔.๕ รองรับมาตรฐานการเชื่อมต่อแบบ ODBC และ JDBC

๔.๖ รองรับการนำโปรแกรมที่พัฒนาด้วยภาษา R และ Python ให้ทำงานและวิเคราะห์ข้อมูลบน บิ๊กดาต้าคลัสเตอร์ได้

๔.๗ สามารถบริหารจัดการทรัพยากร (Resource management) ของงานในคลัสเตอร์ ด้วย YARN ได้เป็นอย่างน้อย

๔.๘ ส่วนจัดการการตั้งค่าของระบบ (System configuration) สามารถบริหารจัดการ คลัสเตอร์ได้อย่างสะดวก ผ่านทาง web-based application

๔.๙ ส่วนติดตามการทำงานของกิจกรรม (Activity monitor) สามารถติดตามสถานะของกิจกรรมหรืองานของระบบ และช่วยแจ้งเตือนผู้ดูแลระบบได้ทราบถึงปัญหาข้อขัดข้องที่เกิดขึ้นได้ ได้แก่ YARN Hive query และ Impala query ได้เป็นอย่างน้อย

๔.๑๐ ส่วนบริหารจัดการทรัพยากรของระบบ (Resource management service) สามารถแสดงสถานะของการใช้งานทรัพยากรของระบบ ได้แก่ หน่วยประมวลผล (CPU) หน่วยความจำหลัก (Memory) และ HDFS ได้เป็นอย่างน้อย

๔.๑๑ มีบริการจัดการกระแสงาน (Job workflow) และตารางการทำงาน (Job scheduler) โดยใช้ Apache Oozie ได้เป็นอย่างน้อย

๔.๑๒ มีระบบสำรองและกู้คืนข้อมูล (Backup and recovery) แบบ HDFS ได้

๔.๑๓ มีระบบรักษาความปลอดภัย (Security system) ขั้นสูง โดยประกอบด้วย ระบบยืนยันบุคคล (User authentication) ด้วยบริการ Kerberos ระบบกำหนดสิทธิผู้ใช้ (User authorization) ด้วยบริการ Active Directory และการเข้ารหัสข้อมูล (Data encryption) ที่รับส่งผ่านระหว่างโหมด ได้เป็นอย่างน้อย

ผนวก ข
รายการคุณลักษณะเฉพาะของระบบบริหารข้อมูลขนาดใหญ่

เครื่องมือบริหารจัดการข้อมูลขนาดใหญ่ แบ่งออกเป็น ๕ ส่วนหลัก ดังนี้

๑. เครื่องมือเชื่อมโยงข้อมูลเข้าสู่แพลตฟอร์มบิ๊กดาต้าแบบเรียลไทม์ (Real-time Big Data Integration)

ชุดซอฟแวร์เพื่อเป็นเครื่องมือใช้สำหรับการเชื่อมโยงข้อมูลขนาดใหญ่แบบเรียลไทม์เพื่อการวิเคราะห์ข้อมูลแบบเรียลไทม์ ที่ใช้งานง่ายโดยมีรูปแบบการเขียนโปรแกรมโดยใช้ภาพ (Drag and Drop UI) เพื่อสร้างกระบวนการเชื่อมต่อแหล่งข้อมูลต่างๆ ได้โดยง่ายและสนับสนุนการเชื่อมต่อข้อมูลเข้าสู่ระบบบิ๊กดาต้าแพลตฟอร์มอย่างเต็มรูปแบบ โดยเครื่องมือที่ใช้พัฒนาต้องมีลักษณะทางเทคนิค ดังนี้

๑) สามารถสร้าง native code ได้อัตโนมัติเพื่อใช้กับส่วนบริการ apache spark และ spark streaming

๒) สามารถรองรับการประมวลผลข้อมูลที่รวดเร็วในแบบ high-scale และ in-memory

๓) สามารถทำงานโดยใช้ประโยชน์จากการทำงานแบบ parallel ของ Hadoop ได้ เพื่อการประมวลผลที่รวดเร็ว

๔) รองรับระบบปฏิบัติการ CentOS Linux, OS X, Red Hat Enterprise Linux, Solaris ·SUSE Linux, Ubuntu Linux และ Microsoft Windows

๕) มีส่วนประกอบหรือ Components ต่างๆ สำหรับการทำงานดังนี้

- ส่วนประกอบสำหรับการทำงานกับ Spark บน Hadoop
- ส่วนประกอบสำหรับ cloud SaaS และ storage
- ส่วนประกอบสำหรับฐานข้อมูล
- ส่วนประกอบสำหรับฐานข้อมูลแบบ NoSQL
- ส่วนประกอบสำหรับ data making และ data transformation
- ส่วนประกอบสำหรับ messaging services
- ส่วนประกอบสำหรับการเชื่อมโยง IoT
- ส่วนประกอบสำหรับ Machine Learning

๖) มีตัวเชื่อมหรือ Connectors เพื่อใช้เชื่อมต่อและดึงข้อมูลจากแหล่งเก็บข้อมูลต่างๆ ที่ทันสมัย โดยอย่างน้อยต้องมีตัวเชื่อมเข้าสู่แหล่งเก็บข้อมูลต่างๆ ดังนี้

- ตัวเชื่อมเข้าระบบบิ๊กดาต้า เช่น Amazon Redshift, Amazon DynamoDB, Amazon EMR (including Apache Spark), Apache Hadoop (HBase, HDFS, Hive), Apache Spark, Cassandra, Couchbase, CouchDB, Cloudera Enterprise, Google BigQuery, Hortonworks Data Platform, Microsoft HDInsight, IBM PureData System for Hadoop, MapR, Mapr_DB, MarkLogic, MongoDB, Neo๔J, Pivotal HD, Riak, SAP HANA, Teradata, THD, Vertica เป็นต้น
- ตัวเชื่อมรองรับไฟล์ที่มีฟอร์แมตต่างๆ เช่น SEQ, JSON, RC, ORC และ AVRO เป็นต้น

- ตัวเชื่อมเข้าสู่ระบบฐานข้อมูล และแหล่งแก็บข้อมูล ต่างๆ เช่น Amazon Aurora, Amazon RDS, Amazon Redshift, Amazon S3, AS400, DB2, Derby DB, Exasol, eXist-db, Firebird, Google Storage, Greenplum, H2, HIVE, HSQLDB, Informix, Ingres, InterBase, JavaDB, JDBC, MaxDB, Microsoft OLE-DB, Microsoft SQL Server, MySQL, Netezza, Oracle, ParAccel, PostgresSQL, PostgresPlus, SAP Business Warehouse, SAS, SQLite, Sybase, Sybase IQ, Teradata, VectorWise, Vertica และ Windows Azure Blob Storage เป็นต้น

- ตัวเชื่อมเข้าส่วนบริการแบบ SaaS (Service as a Service) เช่น Marketo, ServiceNow, Salesforce.com and Salesforce Wave, NetSuite, MS CRM & AX, Amazon S3, Amazon SQS, Bonita, Box, Dropbox, ElasticSearch, Google Drive, JIRA, Email (SMTP), FTP/SFTP, LDAP, REST และ Splunk เป็นต้น

- ตัวเชื่อมเข้าสู่ระบบแบบ Packaged Apps เช่น SAP (table extract, BAPI, IDOC), Sugar CRM, Microsoft, Sage X3, CentricCRM, Vtiger CRM และ Open Bravo เป็นต้น

- ตัวเชื่อมสำหรับระบบเทคโนโลยีอื่นๆ เช่น Amazon S๓, Amazon SQS, Bonita, Box, Dropbox, ElasticSearch, GoogleDrive, JIRA, Email, (SMTP), FTP/SFTP, LDAP, REST และ Splunk เป็นต้น

- ตัวเชื่อมเข้าสู่ระบบ Cloud services เช่น Amazon S๓, Azure IoT/Event Hub Consumer, Google Cloud Storage และ Google Pub/Sub Subscriber เป็นต้น

๗) รองรับและสนับสนุนมาตรฐานการส่งข้อความระดับองค์กร (enterprise messaging standards) และ Messaging services เช่น Apache Spark Streaming, Apache Kafka, Amazon Kinesis และ MapR-Streams

๒. เครื่องมือสนับสนุนการตรวจสอบคุณภาพข้อมูล (Data Quality)

ในการปฏิบัติงานกับข้อมูลที่มีจำนวนมากมายมหาศาล หากข้อมูลเหล่านั้นมีข้อมูลที่ไม่มีความสมบูรณ์ปะปนอยู่ด้วย กล่าวคือ มีข้อมูลบางส่วนที่บันทึกในรูปแบบที่ไม่ตรงกับมาตรฐานกลางที่กำหนดไว้ ซึ่งจะส่งผลให้การวิเคราะห์และประมวลผลนั้นผิดพลาด ก่อให้เกิดความเสียหายทั้งทางด้านระยะเวลาและงบประมาณอย่างมาก

ระบบ **Data quality** เป็นเครื่องมือที่จะทำการคัดกรองข้อมูล ที่มีรูปแบบไม่ตรงตามที่มาตรฐานการเก็บข้อมูลของระบบบิ๊กดาต้า ที่กำหนดไว้ออกมาในรูปแบบของรายงานสถิติ เพื่อทำ Data cleansing ต่อไป โดยเครื่องมือที่ใช้ในการตรวจสอบคุณภาพข้อมูลต้องมีคุณลักษณะ ดังนี้

๑) ตรวจจับข้อมูลที่ซ้ำ (Duplicated) เพื่อทำการลบหรือแยกออกจากระบบบิ๊กดาต้าแพลตฟอร์ม เช่น เลขบัตรประชาชนซ้ำในระบบ เป็นต้น

๒) ตรวจสอบความถูกต้องของข้อมูล (Validation) เพื่อยืนยันความน่าเชื่อถือของระบบบิ๊กดาต้าแพลต ฟอร์ม เช่น หมายเลขไปรษณีย์ที่อยู่ในระบบได้รับการตรวจสอบแล้วว่าเป็นหมายเลขที่มีอยู่จริง เป็นต้น

๓) แจ้งข้อมูลที่ไม่ตรงกับรูปแบบที่กำหนด เช่น หมายเลขโทรศัพท์ต้องอยู่ในรูปของ XXXXXXXXXX เท่านั้น เป็นต้น

๔) สามารถ Export code เพื่อความสะดวกในการนำไป ปฏิบัติการ Data Quality บนระบบปฏิบัติการอื่นๆ เช่น Windows, macOS เป็นต้น ได้ทุกที่

๕) เพิ่มสักยภาพเรื่องความน่าเชื่อถือทางสถิติข้อมูล ให้แก่ระบบระบบบิ๊กดาต้าแพลตฟอร์ม

๖) สามารถรองรับระบบปฏิบัติการ OS X, Windows, Linux based systems, Solaris ได้เป็นอย่างดี

๗) รองรับการเชื่อมต่อกับ Database ภายนอกที่เป็นที่นิยม เช่น Amazon Aurora, Amazon RDS, Amazon Redshift, Amazon S3, AS400, Bonita, Sybase IQ, Box, DB2, Derby DB, Dropbox, EXASOL, eXist-db, Firebird, Google Drive, Google Storage, Greenplum, H2, HSQLDB, Informix, Ingres, InterBase, JavaDB, JDBC, LDAP, MariaDB, MaxDB, Microsoft OLE-DB, Microsoft SQL Server, MySQL, Netezza, Oracle, ParAccel, PostgresSQL, PostgresPlus, SAP Business Warehouse, SAP Hana, SAS, SQLite, Sybase, Sybase IQ, Teradata, VectorWise, Vertica, Windows Azure Blob Storage

๘) รองรับการเชื่อต่อกับระบบ Software-as-a-Service เช่น Marketo, Saleforce Wave เป็นต้น เพื่อเสริมประสิทธิภาพของ application ที่ถูกพัฒนาบนระบบ cloud service ให้สามารถทำงานร่วมกับ Talend data quality ได้

๙) รองรับการเชื่อมต่อกับระบบฐานข้อมูลของบิ๊กดาต้า เช่น Apache Hadoop, Apache Spark เป็นต้น

๑๐) รองรับการเชื่อมต่อกับระบบฐานข้อมูลแบบ NoSQL เพื่อขยายข้อจำกัดในประเภทการเก็บข้อมูลของระบบฐานข้อมูล เช่น AWS DynamoDB, MongoDB เป็นต้น

๑๑) สามารถทำการตรวจสอบความถูกต้องของข้อมูล Data validation ร่วมกับระบบฐานอื่น เช่น สามารถเชื่อมต่อกับระบบฐานข้อมูลที่อยู่กับ Google เพื่อทำการยืนยันที่อยู่ภายใน Database ของเราว่าเป็นที่อยู่ที่มีอยู่จริงหรือไม่ได้ เป็นต้น Amazon Redshif, DynamoDB, EMR (including Apache Spark), Apache Hadoop (HBase, HDFS, Hive), Apache Spark, Cassandra, Couchbase, CouchDB, Cloudera Enterprise, Google BigQuery, Hortonworks Data Platorm, Microsof HDInsight

๓. เครื่องมือสนับสนุนบูรณาการฐานข้อมูลร่วมและแอปพลิเคชัน (ESB & Application Integration)

ระบบฐานข้อมูลบิ๊กดาต้านั้นจะบรรจุข้อมูลที่มีความสำคัญต่อหลายหน่วยงานทั้งภายในและภายนอกหน่วยงานนั้นๆ ดังนั้นความสามารถของตัวระบบที่ต้องรองรับ การเข้าใช้งานบริการทางข้อมูลด้วยอุปกรณ์ที่มีความหลากหลาย เช่น ผ่านระบบ Windows, OS X, mobile apps เป็นต้น และต้องสามารถเชื่อมต่อตัวระบบเองกับระบบ บิ๊กดาต้า ขององค์กรภายนอกได้ จึงเป็นปัจจัยที่สำคัญที่ขาดเสียไม่ได้

ESB เป็นเครื่องมือที่สามารถตอบสนองความต้องการ ด้วยความสามารถในการบูรณาการข้อมูลร่วมกับฐานข้อมูลขององค์กรอื่นๆ และรองรับการเข้าถึงระบบจากอุปกรณ์ต่างๆผ่าน Internet โดยมีคุณลักษณะดังนี้

๑) สามารถเชื่อมต่อจากตัวระบบ ESB ร่วมกับระบบฐานข้อมูลอื่นๆ เช่น Amazon RDS, Microsoft SQL server เป็นต้น เพื่อใช้ในการรับส่งข้อมูลได้

๒) ให้บริการในการรับส่งข้อมูลจาก platform หนึ่งไปสู่ platform หนึ่งทั้งระบบ on-premises และ cloud ได้อย่างรวดเร็ว

๓) ผู้พัฒนาระบบ developer สามารถสร้างโปรแกรมในการทำงานด้านการตรวจคุณภาพข้อมูล Data quality ที่สามารถนำไป run บนระบบปฏิบัติการอื่นๆ ในรูปแบบของ Java code ได้อย่างง่ายดาย เช่น web service, REST Application, messaging routes เป็นต้น ภายในหน้าจอการทำงาน Interface เดียว

๔) แสดงโครงสร้างการเชื่อต่อฐานข้อมูลที่มีความซับซ้อนออกมาในรูปแบบของแผนภาพ Diagram ที่ทำให้ผู้ใช้สามารถทำงานหรือศึกษาระบบการเชื่อมต่อได้โดยง่าย

๕) แสดงสถิติการตรวจจับและคัดกรองข้อมูลออกมาในรูปแบบรายงานเชิงสถิติ ซึ่งง่ายต่อผู้ไม่มีพื้นฐานทาง IT ในการศึกษา

๖) มี API หรือชุดคำสั่งที่ระบบอื่นสามารถนำไปใช้เชื่อมต่อกับการทำงานอื่นๆในขีดความสามารถของ ESB ได้ เช่น ระบบ web app สามารถเชื่อมต่อกับ ESB ผ่าน API ของตัว ESB เพื่อเข้าไปรับข้อมูลต่างๆในระบบได้ เป็นต้น

๗) รองรับช่องทางการรับส่งข้อมูลได้หลาย Format เช่น JSON, XML เป็นต้น

๘) รองรับภาษาโปรแกรมที่ใช้ในการเขียน Script เช่น Groovy, Javascript, PHP, Ruby

๙) สนับสนุนการเชื่อมต่อกับ Database ต่างๆ เช่น Microsoft SQL Server, MongoDB, Oracle, MySQL เป็นต้น

๑๐) สามารถทำงานได้บนระบบปฏิบัติการ Linux based system, Windows, OS X, Solaris

๔. เครื่องมือสนับสนุนการบริการจัดการ Data Catalog

Data Catalog จัดระเบียบข้อมูลของคุณเพื่อควบคุมการเข้าถึง และได้ใช้งานข้อมูลที่เชื่อถือได้จากแหล่งเดียวกัน ธุรกิจต่าง ๆ สามารถที่จะค้นหาข้อมูลที่ถูกต้องได้อย่างรวดเร็ว เจ้าหน้าที่ผู้รับผิดชอบข้อมูลสามารถที่จะติดตามข้อมูลเพื่อเพิ่มศักยภาพในการกำกับดูแลและความเป็นส่วนตัวในการเข้าถึงข้อมูลเพื่อใช้ในการ การค้นหาข้อมูลอัตโนมัติ สร้างและควบคุมแคตตาล็อกข้อมูลส่วนกลาง และยังสามารถการค้นหาและแลกเปลี่ยนข้อมูลได้อย่างรวดเร็ว โดย Data Catalog ควรมีคุณลักษณะดังนี้

ขีดความสามารถ

๑) สามารถรองรับมาตรฐานต่างๆ เช่น OMG Common Warehouse Model, OMG unified Model Language (UML), Open API Specifications (OAS), W3C OWL/RDF, XML & XMI, Ocal Copybooks, SQL

๒) สามารถนำเข้าและบูรณาการข้อมูลและ Scripting เช่น Apache Sqoop, AWS Glue ETL, Informatica Developer, Infomatica Power Center, IRI CoSORT, Microsoft SQL Server SSIS, Oracle Data Integration (ODI), Oracle Warehouse Builder (OWB) Pentaho DI, SAP Data Services (BODI/BODS), SAS Data Integration

๓) สามารถเชื่อมต่อกับเครื่องมือของธุรกิจอัจฉริยะ Business Intelligence Tools ได้ เช่น IBM Cognos, Microsoft Azure Power BI Service, Microsoft SSAS & SSRS, MicroStrategy, Oracle Business Intelligence (OBI), Qlik QlikSense & QlikView, SAP BusinessObjects, SAS Visual Analytics, Tableau, Tibco Spotfire

๔) สามารถเชื่อมต่อเข้ากับ Metadata Management solutions ได้ เช่น Cloudera Navigator, Hotonwroks Atlas, Metadata Excel Format

๕) สามารถเชื่อมต่อกับ Data Modeling Tools ได้ เช่น CA Component Modeler, Erwin Data Modeler, IBM InfoSphere Data Architect, IBM Rational Rose, IBM Telelogic Tau, IDERA ER/Studio, Microsoft Visio, Microsoft Visual Studio/Modeler, No Magic Magic Draw, Oracle Data Modeler (ODM), Oracle Designer, SAP Power Designer, Sparx Enterprise Architect (EA), Tigris ArgoUML, Unicom (Popkin), Visible IE Advantage

๖) สามารถเชื่อมต่อกับ Database Metadata Connectors ได้ เช่น Amazon RedShift Database, HP Vertica Database, IBM DB๒, IBM Lotus Notes, IBM Netezza Database, Oracle Database & PL/SQL, Oracle hyperion Essbase, Oracle MySQL Database, PostgreSQL Database, SAP HANA Database, SAP NetWeaver MDM, SAP Sybase ASE Database, Snowflake, SQL Server Database, Teradata Database

๗) สามารถเชื่อมต่อกับ Hadoop, File Systems และ NoSql ได้ เช่น Apache Cassandra NoSQL Database, Apache CouchDb Database (JSON) , Apache HDFS, Apache Hadoop HBase, Apache Hadoop Hive Database, Apache Kafka , AWS Simple Storage Service, Cloudera Impala, DataStax Enterprise (Cassandra), File System (HDFS, S3, CSV, Excel, XML, JSON, Avro, Parquet, ORC, COBOL Copybook), Google BigQuery Database, MarkLogic NoSQL Database, Microsoft Azure Blob Storage, Microsoft Azure SQL Database, Oracle Cloud Object Storage Classic, Pivotal Greenplum Database, Vector (Vectorwise) Database, Windows and Linux File System

๘) สามารถเชื่อมต่อกับ Development และ DevOps ได้ เช่น Altova XML Spy, Borland Together, CA COOL & Gen, EMC ProActivity, Gentleware Poseidon

๕. เครื่องมือสนับสนุนการบริหารจัดการข้อมูลหลัก (Master Data Management)

ชุดซอฟแวร์ที่ทำหน้าที่บริหารจัดการข้อมูลทั้งหมดของระบบตั้งแต่ขั้นตอนรวบรวมข้อมูลจากแหล่งข้อมูล (Collect) ขั้นตอนบริหารจัดการและธรรมาภิบาลข้อมูล (Govern) ขั้นตอนการปรับปรุงเปลี่ยนแปลงข้อมูล (Transform) และขั้นตอนการแบ่งปันแลกเปลี่ยนข้อมูล (Share) เพื่อควบคุมติดตามการดำเนินงานด้านข้อมูลเป็นไปอย่างน่าเชื่อถือและรวดเร็วตั้งแต่ต้นทางแหล่งข้อมูลผ่านตัวเชื่อม (Data Source : Data Connector) ไปยังปลายทางคือกลุ่มเป้าหมายผู้ใช้งานข้อมูลผ่าน api (Target Data : Service Api) โดยเครื่องมือที่ใช้พัฒนาต้องมีลักษณะทางเทคนิค ดังนี้

๑) รองรับระบบปฏิบัติการ CentOS Linux, OS X, Red Hat Enterprise Linux, Solaris ·SUSE Linux, Ubuntu Linux และ Microsoft Windows

๒) รองรับตัวเชื่อมเข้าสู่ระบบฐานข้อมูล และแหล่งแก็บข้อมูล ต่างๆ เช่น Amazon Aurora, Amazon RDS, Amazon Redshift, Amazon S3, AS400, DB2, Derby DB, Exasol, eXist-db, Firebird, Google Storage, Greenplum, H2, HSQLDB, Informix, Ingres, InterBase, JavaDB, JDBC, MariaDB, MaxDB, Microsoft OLE-DB, Microsoft SQL Server, MySQL, Netezza, Oracle, ParAccel, PostgresSQL, PostgresPlus, SAP Business Warehouse, SAS, SQLite, Sybase, Teradata, VectorWise, Vertica และ Windows Azure Blob Storage เป็นต้น

๓) รองรับส่วนบริการแบบ SaaS (Service as a Service) และ 3rd Party Application เช่น Alfresco, Centric CRM, ElasticSearch, JIRA, Marketo, Microsoft CRM and AX, NetSuite, Open Bravo, SAGE X3, Salesforce.com, Salesforce Wave, SAP, Splunk, ServiceNow, SugarCRM และ Vtiger CRM เป็นต้น

๔) รองรับการทำงานตรวจสอบโดยใช้ Matching Algorithms ต่างๆ เช่น Exact Match, SoundEx, Soundex FR, Metaphone, Double Metaphone, Levenshtein, Jaro, Jaro-Winkler, Q-gram และ Custom/User-Defined เป็นต้น

๕) รองรับการทำ Master Data Repository และจัดเก็บ Master Data บนระบบ RDMS ที่รองรับได้ เช่น Exact Match, SoundEx, Soundex FR, Metaphone, Double Metaphone, Levenshtein, Jaro, Jaro-Winkler, Q-gram และ Custom/User-Defined เป็นต้น

๖) รองรับการผูกข้อมูล (Bindings) ที่มีคุณสมบัติดังนี้

- รูปแบบต่างๆ เช่น SOAP และ REST/HTT เป็นต้น
- ประเภทต่างๆ เช่น Aegis, JAXB 2.2, SDO, XMLBeans และ JIBX เป็นต้น
- ฟอร์แมตต่างๆ เช่น XML และ JSON เป็นต้น
- Protocols ต่างๆ เช่น HTTP, Servlet, JMS, MQTT, AMQP, UDP, Apache Kafka, SMTP/IMAP/POP3, TCP, Jabber, CometD และ WebSocket เป็นต้น

ผนวก ค
รายการคุณลักษณะเฉพาะของระบบ Data Visualization

ซอฟท์แวร์ สำหรับ Data Visualization โดยมีคุณสมบัติดังนี้

๑. ซอฟต์แวร์สำหรับผู้พัฒนาระบบและดูแลระบบ (License Desktop) จำนวน ๕ ชุด โดยมีคุณสมบัติดังนี้

๑.๑ รองรับการเชื่อมต่อกับแหล่งข้อมูลที่มีความหลากหลาย ซึ่งประกอบด้วย แหล่งข้อมูลที่เป็นไฟล์ เช่น Hive๒ บน Big Data Hadoop, Excel, Access, flat files, แหล่งข้อมูลที่เป็น direct SQL ad-hoc querying เช่น SQL Server, Oracle

๑.๒ รองรับการเชื่อมต่อกับแหล่งข้อมูลทั้งในรูปแบบ live connection และ extraction

๑.๓ มีระบบ Memory Optimization รองรับการดึงข้อมูล (Extracted data) โดยเก็บข้อมูลไว้ในหน่วยความจำ (memory) ในลักษณะ Dynamic โดยไม่จำเป็นที่จะต้องเก็บข้อมูล (Extract data) ทั้งหมดเอาไว้ในหน่วยความจำ

๑.๔ รองรับการดึงข้อมูลและคำนวณผลรวมของข้อมูล (Data Extraction and Aggregation) โดยที่ไม่ต้องเขียนโปรแกรมหรือสคริปท์ใดๆทั้งสิ้น

๑.๕ สามารถที่จะรวมข้อมูลจากหลายแหล่งข้อมูลโดยรวมถึงข้อมูลไฟล์ (xls, csv, txt, etc) ในเครื่องของผู้ใช้งานเองเพื่อนำมาวิเคราะห์ร่วมกัน

๑.๖ ผู้ใช้งานสามารถที่จะเชื่อมต่อแหล่งข้อมูลได้โดยง่าย โดยไม่ต้องเขียนสคริปท์ใดๆ

๑.๗ สามารถที่จะสร้างรูปแบบการดึงข้อมูลที่เป็น custom extraction routine โดยใช้ Extraction API ได้

๑.๘ การเชื่อมต่อกับแหล่งข้อมูลหลายๆแหล่ง เชื่อมต่อกับแหล่งข้อมูลหลายๆแหล่งพร้อมๆกันเพื่อทำ data meshing และ data blending ได้

๑.๙ ผู้ใช้งานสามารถจัดเรียงข้อมูลได้โดยอัตโนมัติหรือการจัดเรียงแบบ manual บนกราฟ (visual graphs) ต่างๆได้

๑.๑๐ ผู้ใช้งานสามารถ pivot หรือ drill ในมิติ (dimensions) อื่นๆได้ (เป็นการ drag & drop หรือ expanding and collapsing สำหรับการ drill-down)

๑.๑๑ ผู้ใช้งานสามารถกำหนด thresholds โดยค่าที่มากกว่า threshold จะถูกไฮไลท์ (เช่น red bold font, colors, shapes in chart)

๑.๑๒ ข้อมูล Tooltip จะถูกแสดงเมื่อผู้ใช้งาน วางเมาส์ (hovering) บนพื้นที่ต่างๆเช่น แผนที่ (map), แผนภูมิ (chart), ตาราง (table) หรือรายงาน (report)

๑.๑๓ Data Visualization จะต้องสามารถสร้างแผนภูมิ (charts) ตามข้อมูลที่ถูกเลือกได้ อย่างน้อยดังนี้

- ๑.๑๓.๑ Bar Charts
- ๑.๑๓.๒ Hilight Tables
- ๑.๑๓.๓ Line Charts
- ๑.๑๓.๔ Scatter Plots
- ๑.๑๓.๕ Heat Maps
- ๑.๑๓.๖ Gantt Bar Charts

๑.๑๓.๗ Pie Charts

๑.๑๓.๘ Treemaps

๑.๑๓.๙ Box Plots

๑.๑๓.๑๐ Packed Bubble Charts

๑.๑๓.๑๑ Map Views

๑.๑๔ รองรับ Geospatial Data รองรับข้อมูลในรูปแบบ Geospatial และทำการ สร้างแลตติจูด (Latitude) และ ลองติจูด (Longitude) ของประเทศไทย และจังหวัดโดยอัตโนมัติและไม่ต้องเขียนโปรแกรมหรือสคริปท์ใดๆ ทั้งสิ้น

๑.๑๕ ต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์หรือสาขาผู้ผลิตในประเทศไทย

๑.๑๖ เป็นผลิตภัณฑ์จากประเทศยุโรปหรืออเมริกาเท่านั้น

๑.๑๗ สามารถที่จะแสดงข้อมูลไปบนภาพ (Background Image) ที่เป็นโครงสร้างที่ออกแบบไว้เช่น แผนที่ประเทศ, แผนที่นั่งสนามกีฬา (stadium seating), แผนผังร้านค้า (store layout), แผนผังที่นั่งเครื่องบิน (airplane diagram) เป็นต้น

๑.๑๘ สามารถที่จะแสดงรูปทรงที่ต่างกัน (graphically different shapes) บนแผนที่ได้

๑.๑๙ ใช้งานสามารถที่จะปรับเปลี่ยนรูปแบบ filter ได้ในหลายๆ แบบดังต่อไปนี้

๑.๑๙.๑ Single Value Radio Button

๑.๑๙.๒ Single Value Dropdown

๑.๑๙.๓ Single Value Slider

๑.๑๙.๔ Multiple Value Checkbox

๑.๑๙.๕ Multiple Value Dropdown

๑.๑๙.๖ Multiple Value Custom List

๑.๑๙.๗ Multiple Value Wildcard Search List

๑.๒๐ รองรับ Drag and Drop Dashboard Design สามารถที่จะรวมทุก worksheets เพื่อนำไปใส่ใน dashboard โดย drag & drop worksheets ไปยัง dashboard ได้

๑.๒๑ รองรับ Interactive Story Telling สามารถที่จะจับประเด็นข้อมูลสำคัญ (key insights) โดยใช้ annotations, highlights และ filters ได้ นอกจากนี้ยังสามารถเพิ่มการอธิบาย (descriptions) เพื่อเน้นสิ่งที่เราพบ ทั้งนี้จะทำให้การเล่าเรื่องราว (story) เป็นลักษณะ interactive และก่อให้ เกิดการค้นหาต่อไปได้

๑.๒๒ รองรับการทำงานบน Window และ MAC OS ใน ผลิตภัณฑ์ desktop

๑.๒๓ ซอฟต์แวร์สำหรับผู้พัฒนาระบบและดูแลระบบ (License Desktop) จะต้องเป็นผู้ผลิตยี่ห้อเดียวกันกับซอฟต์แวร์สำหรับเครื่องแม่ข่ายและแสดงผลสำหรับนักวิเคราะห์ (License Server)

๒. ซอฟต์แวร์สำหรับเครื่องแม่ข่ายและแสดงผลสำหรับนักวิเคราะห์ (License Server) จำนวน ๑ ชุด (๑๐ ผู้ใช้งาน) โดยมีคุณสมบัติดังนี้

๒.๑ สามารถส่งข้อมูลการวิเคราะห์ (analytic content) ไปยังผู้ใช้งานใน รูปแบบ on-demand และรูปแบบ schedule ได้ โดยผู้ใช้งานสามารถ subscribe เพื่อที่จะรับ dashboards ทาง email ตามตารางเวลาที่กำหนดไว้ ซึ่งภายใน email จะมี link ไปสู่ online dashboard ด้วย

๒.๒ ระบบจะต้องรองรับการเขียนเนื้อหา (content authoring) บน web browser โดยที่ไม่ต้องใช้โปรแกรม Desktop

๒.๓ ระบบจะต้องรองรับ web browser มาตรฐานต่างๆ ในเวอร์ชั่นเท่ากันหรือสูงกว่า ดังนี้ I.E 8, Firefox 3.x, Android Browser 3.2, Safari 3.x, iOS 5.1.1, Google Chrome

๒.๔ ระบบจะต้องรองรับการใช้งานใน mobile devices มาตรฐานเช่น Apple หรือ Android devices ผ่าน device browser และ native mobile app

๒.๕ การเข้าใช้งานระบบสามารถรองรับการต่อเชื่อมเข้ากับ Active Directory หรือ SAML 2.0 เพื่อทำการ single sign-on ได้

๒.๖ ผลิตภัณฑ์ต้องรองรับการทำงานแบบ automatic clustering เพื่อ high availability และ failover

๒.๗ การเข้าถึงข้อมูล (Data Access) จะถูกกำหนดสิทธ์โดยหน้าที่ (roles), กลุ่ม (groups) หรือประเภทของผู้ใช้งาน (user types)

๒.๘ สามารถทำงานแบบ Multi-tenancy โดยสามารถแบ่งเป็นหลาย sites, workspaces, content, users และ workbooks ได้ โดยที่ยังใช้ Server เดียว (one instance of server) นอกจากนี้สมาชิกของในแต่ละ site จะไม่เห็นข้อมูลของ site อื่นๆใน server เดียวกัน

๒.๙ ข้อมูลที่ถูกส่งผ่าน Internet จะต้องเป็นไปตาม security guideline โดยสามารภทำการ encryption ได้

๒.๑๐ ผู้ควบคุมระบบสามารถดูรายงาน (reports) สถิติการใช้งานของ report และ dashboard ได้

๒.๑๑ ต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายจากเจ้าของผลิตภัณฑ์หรือสาขาผู้ผลิตในประเทศไทย

๒.๑๒ เป็นผลิตภัณฑ์จากประเทศยุโรปหรืออเมริกาเท่านั้น

๒.๑๓ ผู้ควบคุมระบบสามารถดูรายงาน (reports) ที่เป็นสถิติการใช้งานของผู้ใช้ (user activity statistics) ได้

๒.๑๔ รองรับการทำงานแบบ ๖๔-bit

๒.๑๕ ผลิตภัณฑ์สามารถทำงานได้กับข้อมูลหลายภาษา

ผนวก ง

รายการคุณลักษณะเฉพาะของระบบแสดงผลการวิเคราะห์และแจ้งเตือน เพื่อความมั่นคงแห่งชาติ ๓๖๐° (National Security Analytics and Notifications 360°)

ระบบแสดงผลการวิเคราะห์และแจ้งเตือนเพื่อความมั่นคงแห่งชาติ ๓๖๐° (National Security Analytics and Notifications 360°) มีคุณลักษณะเฉพาะดังนี้

๑. คุณลักษณะทางเทคนิคของระบบระบบแสดงผลการวิเคราะห์และแจ้งเตือนเพื่อความมั่นคงแห่งชาติ ๓๖๐°

๑.๑ ระบบต้องสามารถรองรับการนำเสนอรายงาน และ dashboard ในแบบเชิงโต้ตอบ (Interactive dashboards) ผ่านเว็บและเครื่องมืออุปกรณ์มือถือแบบ Smart phone

๑.๒ ระบบต้องสามารถเชื่อมต่อกับระบบธุรกิจอัจฉริยะหรือ Business Intelligence (BI) Server ที่ใช้จัดเก็บรายงานและ Dashboards ต่างๆ เพื่อนำเสนอรายงานบนเว็บและ Mobile App ได้

๑.๓ ระบบต้องสามารถแสดงและนำเสนอข้อมูล Data Visualization ที่เป็นรูปแผนภูมิ (Charts) ได้ทุกแผนภูมิ เช่นเดียวกับขีดความสามารถที่ระบบ Business Intelligence สามารถทำได้ เช่น Bar Charts, Bubble Charts, Hilight Tables, Line Charts, Scatter Plots, Heat Maps, Gantt Bar Charts, Pie Charts, Treemaps, Box Plots, Packed Bubble Charts และ Map Views เป็นต้น

๑.๔ ระบบต้องมีขั้นตอนการยืนยันตัวตน (Authenication) และระบบการอนุญาต (Authorization) ที่ได้มาตรฐาน

๑.๕ ระบบต้องสามารถกำหนดการเข้าใช้ กำหนดสิทธิ์และบริหารจัดการผู้ใช้ระบบ ได้หลายระดับชั้นหลายกลุ่มและประเภทผู้ใช้ หรือตามระดับชั้นความลับของข้อมูล

๑.๖ ระบบต้องมีขีดความสามารถ ในการกำหนดสิทธิ์การเข้าถึงรายงาน และ dashboard ได้ตามประเภทหรือกลุ่มผู้ใช้งาน และต้องสามารถเลือกใช้การกำหนดสิทธิ์ จากระบบแม่ข่ายธุรกิจอัจฉริยะ หรือ Business Intelligence Server ได้ถ้ามี

๑.๗ ข้อมูลที่ถูกส่งผ่าน Internet จะต้องเป็นไปตาม Security guideline โดยมีการเข้ารหัสข้อมูล Data encryption ในระหว่างที่ส่งผ่านข้อมูล

๑.๘ ระบบจะต้องรองรับ Web browser มาตรฐานต่างๆ ในเวอร์ชันเท่ากันหรือสูงกว่า ดังนี้ Microsoft Edge 17.x, Firefox 3.x, Android Browser 3.2, Safari 3.x, iOS 5.1.1 และ Google Chrome

๑.๙ ระบบจะต้องรองรับการใช้งานใน Mobile devices มาตรฐานเช่น Apple และ Android ผ่าน Device browser และ Native mobile app

๑.๑๐ ระบบจะต้องสามารถสร้าง กำหนดรูปแบบ กำหนดเงื่อนไข และส่งข้อความและข้อมูลการแจ้งเตือนแบบ (Push Notifications) ไปยัง Mobile Apps ได้ตามเงื่อนไข กฎและข้อกำหนดของข้อมูลได้แบบทันที (Real-time)

๑.๑๑ ระบบต้องมีการบริหารจัดการสิทธิ์ผู้ใช้เพื่อรับหรือไม่รับข้อความแจ้งเตือนได้ตามประเภท กลุ่มหรือระดับของผู้ใช้ได้เช่นเดียวกับการกำหนดสิทธิ์การเข้าถึงรายงานและ dashboard

๑.๑๒ ระบบต้องมี Agent ในการทำหน้าที่แจ้งเตือนเฉพาะของแต่ละการแจ้งเตือน และมีการพัฒนาตัว Agent แบบ Microservice ที่แต่ละ Agent สามารถทำงานเองเป็นเอกเทศ โดยไม่พึ่งพาซึ่งกันและกัน แต่สามารถติดต่อสื่อสารกันได้ผ่าน Web service

๑.๑๓ ระบบต้องสามารถบริหาร จัดการและควบคุม Notification Agent Microservices แบบรวมศูนย์ และสามารถดัดแปลงและแก้ไข เงื่อนไขต่างๆสำหรับการส่งข้อความแจ้งเตือน เช่น แจ้งเตือนเมื่อ เงื่อนไขระดับความเสี่ยงที่จะเกิดเหตุ มีการเปลี่ยนแปลงเป็นระดับ ๔ เป็นต้น

๑.๑๔ ระบบการ Authorization/Authenthication และระบบจัดการผู้ใช้ กลุ่มผู้ใช้ และสิทธิ์ผู้ใช้ต่างๆ ต้องสามารถทำงานร่วมกับระบบจัดการผู้ใช้บน Active Directory ของสำนักงานสภาความมั่นคงแห่งชาติได้

๑.๑๕ ระบบการติดต่อสื่อสารระหว่าง Microservice Agent และระบบอื่นๆที่ใช้ Web service จะต้องผ่านมาตรฐาน OAuth๒ เป็นอย่างน้อยสำหรับการยืนยันตัวตน และจัดการสิทธิ์

ผนวก จ

รายการข้อมูลด้านความมั่นคง และข้อมูลที่เกี่ยวข้องกับความมั่นคง ที่ได้จัดเก็บ/มีแผนที่จะจัดเก็บ ในระบบฐานข้อมูลของหน่วยงานต่าง ๆ ในขั้นต้น

ลำดับ	ชื่อข้อมูล/ฐานข้อมูล	หน่วยงาน	หมายเหตุ
๑.	ข้อมูลทะเบียนราษฎร	กรมการปกครอง	
๒.	ข้อมูลทะเบียนอาวุธปืน	กรมการปกครอง	
๓.	ข้อมูลทะเบียนบ้าน	กรมการปกครอง	
๔.	ข้อมูลบัตรประจำตัวประชาชน	กรมการปกครอง	
๕.	ข้อมูลการเปลี่ยนแปลงชื่อตัว-ชื่อสกุล	กรมการปกครอง	
๖.	ข้อมูลทะเบียนสมรส	กรมการปกครอง	
๗.	ข้อมูลบัตรประจำตัวผู้ไม่มีสถานะทางทะเบียน	กรมการปกครอง	
๘.	ข้อมูลทะเบียนบุคคลต่างด้าว	กรมการปกครอง	
๙.	ข้อมูลบัตรประจำตัวผู้ไม่มีสัญชาติไทย	กรมการปกครอง	
๑๐.	ข้อมูลบัตรประจำตัวแรงงานต่างด้าว	กรมการปกครอง	
๑๑.	ข้อมูลภาพใบหน้าคนต่างด้าว	กรมการปกครอง	
๑๒.	ข้อมูลภาพนิ้วมือคนต่างด้าว	กรมการปกครอง	
๑๓.	ข้อมูลที่อยู่บุคคลทุกประเภท	กรมการปกครอง	
๑๔.	ระบบสารสนเทศด้านการข่าว	กอ.รมน.	
๑๕.	ระบบสารสนเทศข่าวกรอง	กอ.รมน. ภาค ๔ สน.	
๑๖.	ข้อมูลสภาพแวดล้อมทางทะเล	ศรชล.	
๑๗.	ข้อมูลสถานการณ์ทางทะเล	ศรชล.	
๑๘.	ข้อมูลเรือประมง	ศรชล.	
๑๙.	ข้อมูลเรือสินค้า	ศรชล.	
๒๐.	ข้อมูลคดีประมงผิดกฎหมาย	กรมประมง	
๒๑.	ข้อมูลสรรพกำลัง	กระทรวงกลาโหม	
๒๒.	ระบบฐานข้อมูลคดี (POLIS)	สำนักงานตำรวจแห่งชาติ	
๒๓.	ข้อมูลหมายจับ	สำนักงานตำรวจแห่งชาติ	
๒๔.	ข้อมูลทะเบียนประวัติอาชญากรรม	สำนักงานตำรวจแห่งชาติ	

ลำดับ	ชื่อข้อมูล/ฐานข้อมูล	หน่วยงาน	หมายเหตุ
๒๕.	ข้อมูลการผ่านแดนคนไทย และคนต่างด้าว	สำนักงานตรวจคนเข้าเมือง	
๒๖.	ข้อมูลที่พำนักบุคคลต่างด้าว	สำนักงานตรวจคนเข้าเมือง	
๒๗.	ทะเบียนแรงงานต่างด้าว (กลุ่มบัตรสีชมพู)	กรมการจัดหางาน	
๒๘.	ข้อมูลผู้ต้องหาตามหมายจับคดีพิเศษ	กรมสอบสวนคดีพิเศษ	
๒๙.	ข้อมูลรายการประวัติหนังสือเดินทาง	กรมการกงสุล	
๓๐.	ข้อมูลทะเบียนคดียาเสพติด	สำนักงานป้องกันและปราบปรามยาเสพติด	
๓๑.	ศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (DXC)	กระทรวงยุติธรรม	
๓๒.	ข้อมูลผู้ต้องขัง	กระทรวงยุติธรรม	
๓๓.	ข้อมูลทะเบียนรถยนต์	กรมการขนส่งทางบก	
๓๔.	ข้อมูลใบทะเบียนเรือไทย / ใบอนุญาตใช้เรือไทย	กรมเจ้าท่า	
๓๕.	ข้อมูลคดีประมงผิดกฎหมาย	กรมประมง	
๓๖.	ข้อมูลสถานะแรงงานต่างด้าวในการทำงานบนเรือ	กรมประมง	
๓๗.	ข้อมูลทะเบียนผู้เสียภาษี	กรมสรรพากร	
๓๘.	ข้อมูลทะเบียนผู้มีรายได้น้อย	กระทรวงการคลัง	
๓๙.	ข้อมูลสินค้าเข้า-ออก	กรมศุลกากร	
๔๐.	ข้อมูลของต้องห้าม-ของต้องกำกัด	กรมศุลกากร	
๔๑.	ข้อมูลสถิติการค้าชายแดน	กรมศุลกากร	
๔๒.	ข้อมูลผู้ได้รับผลกระทบจากเหตุความไม่สงบในจังหวัดชายแดนใต้	กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์	
๔๓.	ข้อมูลอัตลักษณ์บุคคล	สถาบันนิติวิทยาศาสตร์	
๔๔.	ข้อมูลนิติวิทยาศาสตร์	สถาบันนิติวิทยาศาสตร์	
๔๕.	ข้อมูลภัยคุกคามด้านไซเบอร์	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	
๔๖.	ข้อมูลเฝ้าระวังเครือข่ายสังคมออนไลน์	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	

ลำดับ	ชื่อข้อมูล/ฐานข้อมูล	หน่วยงาน	หมายเหตุ
๔๗.	ข้อมูลพื้นที่เสี่ยงเกิดภัยพิบัติ	กรมป้องกันและบรรเทาสาธารณภัย	
๔๘.	ข้อมูลแผนการป้องกันและบรรเทาสาธารณภัย	กรมป้องกันและบรรเทาสาธารณภัย	
๔๙.	ระบบฐานข้อมูล Data Center ศอ.บต.	ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้	
๕๐.	ข้อมูลด้านความมั่นคง อื่นๆ	หน่วยงานด้านความมั่นคงอื่นๆ	
๕๑.	ข้อมูลที่เกี่ยวข้องกับความมั่นคง อื่นๆ	หน่วยงานที่มีข้อมูลที่เกี่ยวข้องกับความมั่นคงอื่นๆ	

ผู้ร่วมในการจัดทำเอกสารข้อเสนอ Platform ด้านความมั่นคง

๑. คณะทำงานด้านเทคนิคจัดทำ Platform ด้านความมั่นคง

๑.๑ พล.ต.ณัฐพงษ์ เพราแก้ว	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร	หัวหน้าคณะทำงาน
๑.๒ น.อ.อุกฤษฏ์ รอดสุทธิ	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร	รองหัวหน้าคณะทำงาน
๑.๓ พ.อ.มนตรี สุพิเพชร	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร	คณะทำงาน
๑.๔ พ.อ.กฤษฎาวุฒิ โสภิกุล	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร	คณะทำงาน
๑.๕ น.อ.สืบวงศ์	กระทรวงกลาโหม	คณะทำงาน
๑.๖ พันเอก อดิศัย มีสมพืชน์	กระทรวงกลาโหม	คณะทำงาน
๑.๗ นาย สุชาติ ธานีรัตน์	กระทรวงมหาดไทย	คณะทำงาน
๑.๘ นาย จิรศักดิ์ ตินสุวรรณ	กระทรวงมหาดไทย	คณะทำงาน
๑.๙ นาง สมศรี หอกันยา	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	คณะทำงาน
๑.๑๐ นางสาว จิณห์จุฑา กันตะสุวรรณ	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	คณะทำงาน
๑.๑๑ นาง สุรีพร พรโสภณวิชญ์	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ	คณะทำงาน
๑.๑๒ นาย ภานุวัฒน์ สุขสบาย	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ	คณะทำงาน
๑.๑๓ นาย พิสุทธิ์ วรรณฉัตรสิริ	กรมป้องกันและบรรเทาสาธารณภัย	คณะทำงาน
๑.๑๔ นาย ทวียศ กลิ่นขจร	กรมป้องกันและบรรเทาสาธารณภัย	คณะทำงาน
๑.๑๕ พ.ต.อ.จักรทิพย์ ศตพิมลศักดิ์	สำนักงานตรวจคนเข้าเมือง	คณะทำงาน
๑.๑๖ พ.ต.อ.พงษ์พิเชษฐ์ นิลจันทร์	สำนักงานตรวจคนเข้าเมือง	คณะทำงาน
๑.๑๗ พ.อ.บุญเลิศ สุกใส	กองอำนวยการรักษาความมั่นคงภายในภาค ๔	คณะทำงาน
๑.๑๘ น.อ.สอาด สุมรรคา	กองอำนวยการรักษาความมั่นคงภายในภาค ๔	คณะทำงาน
๑.๑๙ น.อ.สิทธิโรจน์ สมจิตต์	ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล	คณะทำงาน
๑.๒๐ น.อ.จุมพล นาคบัว	ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล	คณะทำงาน
๑.๒๑ นาย เจษฎาพร ธนาอัศวเดช	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงาน
๑.๒๒ นาย นริน เวโรจน์วิววัฒน์	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงาน
๑.๒๓ นาย ติณณภพ เตียวเจริญ	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงาน
๑.๒๔ นายฐาปะนะ แก้วมณี	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงาน
๑.๒๕ นางสาว กรวรรณ คำกรเกตุ	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงาน
๑.๒๖ พ.อ.พงษ์สันติ์ จันทร์สอน	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร	คณะทำงานและเลขานุการ
๑.๒๗ นายรพี โล่ชัยยะกูล	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงานและผู้ช่วยเลขานุการ (๑)
๑.๒๘ นายธิติพงศ์ หนูขำ	สำนักงานสภาความมั่นคงแห่งชาติ	คณะทำงานและผู้ช่วยเลขานุการ (๒)

๒. ผู้ร่วมนำเสนอข้อมูลในการจัดทำเอกสาร

๒.๑ นาย คณิต คงช่วย	สำนักงานปลัดกระทรวงมหาดไทย
๒.๒ นายกิตติศักดิ์ เดชชาญชัย	สำนักงานสภาความมั่นคงแห่งชาติ
๒.๓ นายชัยเกียรติ ทุมรัตน์	สำนักงานสภาความมั่นคงแห่งชาติ
๒.๔ นางสาวรักษิณา มงคลนิมิต	สำนักงานสภาความมั่นคงแห่งชาติ
๒.๕ นางสาวลักษิกา สงวนสุข	สำนักงานสภาความมั่นคงแห่งชาติ
๒.๖ นางสาวภาวิณี ปรีดี	สำนักงานสภาความมั่นคงแห่งชาติ
๒.๗ นางสาว แสงนภา กออุดม	สำนักงานสภาความมั่นคงแห่งชาติ

การดำเนินงานของหน่วยงานที่เกี่ยวกับการจัดทำระบบฐานข้อมูลด้านความมั่นคง

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
๑. กระทรวงมหาดไทย (กรมการปกครอง)	**๑. ระบบการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (LINKAGE CENTER)**	เชื่อมโยงข้อมูล เช่น ข้อมูลอาวุธปืน โรงแรม การถือครองที่ดิน ข้อมูลการศึกษา หมายจับ ข้อมูลคนไทย คนต่างด้าว แรงงานต่างด้าว เป็นต้น รวมฐานข้อมูลที่ใช้งานได้แล้วกว่า ๑๖๐ ฐานข้อมูล จำนวนข้อมูลกว่า ๑,๔๘๐ ล้านรายการ
	๒. ระบบการเชื่อมโยงข้อมูลทะเบียนประวัติราษฎร (IKNO)	เปิดให้ส่วนราชการเชื่อมโยงข้อมูลมาตั้งแต่ปี ๒๕๔๐ ตามมาตรา ๑๕ พ.ร.บ.การทะเบียนราษฎร พ.ศ. ๒๕๓๔ ประกอบด้วยข้อมูลบุคคล ทั้งคนไทย คนต่างด้าว และแรงงานต่างด้าว รูปใบหน้า มีส่วนราชการนำไปใช้งานทั้งการบริการประชาชน เช่น กรมการกงสุล กรมสรรพากร โรงพยาบาล สตช. เป็นต้น
	๓. ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือ (Automated fingerprint identification systems : AFIS)	ตรวจพิสูจน์ยืนยันตัวตนด้วยลายพิมพ์นิ้วมือทั้งลายนิ้วมือแฝง และลายนิ้วมือปกติจากกระดาษและไฟล์ ปัจจุบันใช้งานตรวจพิสูจน์ศพนิรนาม ลายนิ้วมือแฝงคดีต่าง ๆ เป็นต้น โดยมีข้อมูลลายพิมพ์นิ้วมือทั้งคนไทยและคนต่างด้าว กว่า ๑๒๘ ล้านนิ้ว
	๔) ระบบการตรวจพิสูจน์ยืนยันตัวตนด้วยภาพใบหน้า (Face Recognition)	ตรวจพิสูจน์ยืนยันตัวตนด้วยลายภาพใบหน้าโดยจัดเก็บจากการออกบัตร ซึ่งมีข้อมูลลายพิมพ์นิ้วมือทั้งคนไทยและคนต่างด้าว กว่า ๑๘๐ ล้านหน้า

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
๒. กระทรวงกลาโหม (กรมการสรรพกำลังกลาโหม)	**๑. โครงการพัฒนาระบบสารสนเทศเพื่อการระดมสรรพกำลัง**	ระบบสารสนเทศที่สนับสนุนการตัดสินใจและปฏิบัติงานร่วมกันในการระดมสรรพกำลังของหน่วยงานที่เกี่ยวข้องทั้ง ๑๐ ด้าน โดยระบบงานสามารถวิเคราะห์และประเมินผลเชิงพื้นที่ (Spatial Analysis) เช่น การคำนวณและแสดงยอดสรุปรวมจำนวน/ปริมาณทรัพยากรจากแผนที่ดิจิตอล และการบันทึกแผนที่ยุทธการที่สร้างขึ้นในลักษณะแผนที่ส่วนบุคคล และสามารถประเมินผลเชิงเครือข่าย (GIS Service for Network Analysis) เช่น การหาเส้นทางการส่งกำลังที่เหมาะสมซึ่งจะช่วยสนับสนุนการตัดสินใจและการปฏิบัติงานในด้านการระดมสรรพกำลังและการส่งกำลังได้เป็นอย่างดี พร้อมทั้งมีช่องทางในการใช้งานระบบผ่านทาง Smart Mobile Device เพื่อสนับสนุนและติดตามการส่งกำลังในการปฏิบัติภารกิจ
	๒. โครงการพัฒนาระบบสารสนเทศเพื่อการกำลังสำรองและการสัสดี ***อยู่ระหว่างขออนุมัติโครงการ**	ระบบสารสนเทศฐานข้อมูลกำลังพลสำรองแห่งชาติ สำหรับเป็นฐานข้อมูลกลางขนาดใหญ่ (Central Big Data) ในการรวบรวม สืบค้น และจัดการข้อมูลกำลังพลสำรองแห่งชาติ และเป็นศูนย์กลางข้อมูลกำลังพลสำรองสำรองแห่งชาติในการวางแผน กำหนดยุทธศาสตร์ อำนวยการ และกำกับดูแลข้อมูลกำลังพลสำรองแห่งชาติ

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
๓. สำนักงานตำรวจแห่งชาติ **๓.๑ สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.)**	• **ระบบการสืบค้นข้อมูลหมายจับ ในรูปแบบเว็บเซอร์วิส (Web Service)**	เชื่อมโยงข้อมูลดังกล่าวผ่านระบบการบูรณาการฐานข้อมูลประชาชนและบริการภาครัฐ (Linkage Center) ของกรมการปกครองไว้เรียบร้อยแล้ว หากหน่วยงานด้านความมั่นคงใดต้องการเชื่อมโยงและใช้ข้อมูลหมายจับดังกล่าวสามารถขอเชื่อมโยงข้อมูลจากระบบผ่านระบบการบูรณาการฐานข้อมูลประชาชนและบริการภาครัฐได้โดยตรง
๓.๒ ตำรวจภูธรภาค ๙		เชื่อมโยงกับฐานข้อมูลกลาง สขว.กอ.รมน.ภาค ๔ สน. การเชื่อมโยงต้องได้รับอนุญาตจาก กอ.รมน. ได้แก่ ข้อมูลหมายจับตาม พ.ร.ก.การบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ.๒๕๔๘ ข้อมูลหมายจับตาม ป.วิ อาญาข้อมูลรายชื่อแกนนำร่วม ข้อมูลอาวุธปืนที่ใช้ก่อเหตุ ข้อมูลอาวุธปืนที่สูญหายละได้คืน ข้อมูลอู่ซ่อมรถ/จำหน่ายอะไหล่/รถมือสอง ข้อมูลร้านจำหน่ายโทรศัพท์/ซิมการ์ด ข้อมูลร้านจำหน่ายอุปกรณ์อิเล็กทรอนิกส์และวัสดุก่อสร้าง ข้อมูลวัตถุระเบิดและโรงโม่ และข้อมูลการโจรกรรมรถ

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
๓.๓ สำนักงานตรวจคนเข้าเมือง (สตม.)	**● ข้อมูลแรงงานต่างด้าว ๓ สัญชาติ (เมียนมา ลาว กัมพูชา)**	เชื่อมโยงกับกระทรวงมหาดไทยและกระทรวงแรงงาน
๔. กระทรวงยุติธรรม	**๑. ระบบฐานข้อมูลดีเอ็นเอ**	มีช่องทางสำหรับการเชื่อมโยงข้อมูลแล้ว
	๒. ระบบฐานข้อมูลลายพิมพ์นิ้วมือ	อยู่ระหว่างการปรับประสิทธิภาพของระบบจัดเก็บฐานข้อมูล
	๓. ระบบฐานข้อมูลบุคคลสูญหายและศพนิรนาม	เชื่อมโยงข้อมูลกับระบบศูนย์กลางการแลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center)
	๔. ระบบฐานข้อมูลการตรวจพิสูจน์ทางนิติวิทยาศาสตร์	มีช่องทางสำหรับการเชื่อมโยงข้อมูลแล้ว
๕. สำนักเลขาธิการนายกรัฐมนตรี	**● แผนและขั้นตอนการรับมือภัยคุกคามทางไซเบอร์**	**๑. การวางแผนและเตรียมความพร้อม (Planning and Preparing)** เตรียมเครื่องมือและอุปกรณ์ สำนักเลขาธิการนายกรัฐมนตรี ได้รับความร่วมมือจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (ETDA) ในการจัดเตรียมแผนและความพร้อม โดยจัดให้มีการซักซ้อมในการรับมือภัยคุกคามทางไซเบอร์ ประกอบด้วย การติดต่อสื่อสารและสิ่งอำนวยความสะดวก จัดให้มีอุปกรณ์ และซอฟต์แวร์สำหรับวิเคราะห์เหตุของภัยคุกคามด้วยระบบ Security Information and Event Management (SIEM) ซอฟต์แวร์สำหรับบรรเทาภัยคุกคาม มีการป้องกันเหตุของภัยคุกคาม มีการประเมินความเสี่ยง เป็นระยะๆ จัดให้มีอุปกรณ์ Next Generation Firewall (NGFW) Database Firewall เพื่อการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์แม่ข่าย รวมทั้ง

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายจัดให้มีอุปกรณ์บันทึกข้อมูลการเข้าและออกระบบเครือข่าย (Log) และมีการป้องกันมัลแวร์ด้วย TrendMicro Antivirus เป็นต้น
		๒. การตรวจจับและรายงานผล (Detection and Reporting) การตรวจจับภัยคุกคามหรือเหตุการณ์ไม่ปกติด้านความมั่นคงปลอดภัย มีการรวบรวมข้อมูลและวิเคราะห์ภัยคุกคามหรือเหตุการณ์ไม่ปกติ เพื่อประเมินว่าเป็นเหตุภัยคุกคามจริงหรือไม่ มีรูปแบบการโจมตีอย่างไร มีสัญญาณการเกิดเหตุภัยคุกคาม เช่น จากช่องโหว่บนเครื่องคอมพิวเตอร์แม่ข่ายหรือไม่ โดยใช้เครื่องมือตรวจจับการบุกรุกเครือข่าย
		๓. การประเมินและตัดสินใจ (Assessment and Decision) มีการประเมินและตัดสินใจครั้งสุดท้ายว่า ข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยใดเป็นภัยคุกคาม โดยพิจารณาจากเกณฑ์ในการแบ่งประเภทภัยคุกคาม และระบบสารสนเทศที่ได้ผลกระทบ บันทึกข้อมูลเหตุภัยคุกคาม การวิเคราะห์การจัดระดับความรุนแรงของเหตุภัยคุกคาม โดยพิจารณาจากผลกระทบของการให้บริการ ผลกระทบต่อข้อมูล และความสามารถในการฟื้นฟูระบบ

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		๔. การตอบสนอง (Responses) การตอบสนองต่อเหตุของภัยคุกคาม โดยการปฏิบัติให้สอดคล้องกับผลการพิจารณา ตามขั้นตอนการประเมินและตัดสินใจ โดยแจ้งข้อมูลเหตุภัยคุกคามให้ที่ผู้เกี่ยวข้องรับทราบ มีการควบคุมภัยคุกคาม การรวบรวมและเก็บรักษาพยานหลักฐาน การกำจัดภัยคุกคาม การฟื้นฟูระบบ และการระบุแหล่งที่มาหรือโฮสต์ (Host) ที่โจมตี
		๕. การเรียนรู้จากจากเหตุภัยคุกคาม (Lessons Learned) การเรียนรู้จากเหตุภัยคุกคาม เพื่อปรับปรุงกระบวนการ และการรักษาความมั่นคงปลอดภัย โดยการทบทวนเหตุของภัยคุกคาม และวิธีรับมือกับภัยคุกคามที่เกิดขึ้น
๖. สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม		ได้ดำเนินการตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งมีผลบังคับใช้เมื่อ ๒๘ พ.ค. ๒๕๖๒ โดยมีหลักการสำคัญ คือ การมุ่งที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ การโจมตีระบบหรือโครงข่ายจากอาชญากรคอมพิวเตอร์ที่อาจกระทบต่อการให้บริการแก่ประชาชนหรือความสงบเรียบร้อยภายในประเทศ เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างท่วงที ซึ่งได้กำหนดไว้เป็น ๓ ระดับคือ ระดับเฝ้าระวัง ระดับร้ายแรง ระดับวิกฤติ ที่เกิดขึ้นกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ทั้งหน่วยงานของรัฐและหน่วยงานเอกชน

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		ใน ๘ กลุ่มหลัก ได้แก่ ความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค สาธารณสุข และด้านอื่น ๆ ตามที่คณะกรรมการกำหนดเพิ่มเติม นอกจากนี้ พระราชบัญญัติฯ ได้กำหนดให้มีคณะกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (กมช.) ที่มีนายกรัฐมนตรี เป็นประธาน มีหน้าที่กำหนดนโยบายให้หน่วงของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และยังให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ที่มีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ กำกับดูแลเรื่องภัยคุกคามทางไซเบอร์และความมั่นคง เรื่องมาตรฐานขั้นต่ำของระบบไซเบอร์และส่งเสริมพัฒนา สร้างมาตรฐาน ยกระดับทักษะความรู้ และกำหนดหน้าที่ของ CII และ Regulator เพื่อให้การรับมือกับภัยคุกคามทางไซเบอร์ได้ทันท่วงที ทั้งนี้ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จะทำหน้าที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติเป็นการชั่วคราว ระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ และปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		เลขาธิการจนกว่าจะมีการแต่งตั้ง ทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการ พระราชบัญญัติฯ ฉบับนี้ได้ให้ความสำคัญกับการจัดทำฐานข้อมูลต่าง ๆ ได้กำหนดไว้ชัดเจน โดยให้ดำเนินการพัฒนาระบบฐานข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการป้องกันภัยคุกคามด้านไซเบอร์ในระดับชาติอีกด้วย
๗. ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.)		ดำเนินงานเกี่ยวข้องกับการรักษาผลประโยชน์ของชาติทางทะเลต่อจากศูนย์ประสานการปฏิบัติในการรักษาผลประโยชน์ของชาติทางทะเลภายใต้ พ.ร.บ. การรักษาผลประโยชน์ของชาติทางทะเล พ.ศ. ๒๕๖๒ มีภารกิจหน้าที่เกี่ยวข้องในการรักษาผลประโยชน์ของชาติทางทะเล รวมถึงการ บูรณาการข้อมูลของหน่วยงานของรัฐให้สามารถติดต่อ เชื่อมโยง หรือแลกเปลี่ยนข้อมูลระหว่างกันได้ เพื่อประโยชน์ในการรักษาผลประโยชน์ของชาติทางทะเลหรือกิจกรรมทางทะเล
๘. สำนักงานสถิติแห่งชาติ		จากการดำเนินงานที่ผ่านมาของคณะกรรมการขับเคลื่อนการดำเนินนโยบายเพื่อใช้ประโยชน์ข้อมูลขนาดใหญ่ (Big Data) ศูนย์ข้อมูล (Data Center) และคลาวด์คอมพิวติ้ง (Cloud Computing) พบว่า ปัญหาของการวิเคราะห์ข้อมูลขนาดใหญ่ คือ มีปริมาณข้อมูลที่ถูกผลิตขึ้นอย่างต่อเนื่องจำนวนมาก ทำให้การเลือกใช้ข้อมูลและการสืบค้นหาแหล่งข้อมูลที่เหมาะสมสำหรับการวิเคราะห์หรือให้บริการมีความซับซ้อนและยุ่งยากสูง

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		ดังนั้น เพื่อให้การใช้ประโยชน์ข้อมูลภาครัฐเกิดขึ้นได้อย่างเป็นรูปธรรม จึงมอบหมายให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานสถิติแห่งชาติ วางแผนในการพัฒนารายการข้อมูลภาครัฐ (Government Data Catalog) และระบบสารสนเทศเพื่อการสืบค้นขึ้น เพื่อช่วยให้ผู้ใช้ประโยชน์ข้อมูลสามารถสืบค้นร้องขอเข้าถึงทราบแหล่งที่มาระดับชั้นความลับประเภทรูปแบบและสามารถใช้ประโยชน์ของข้อมูลภาครัฐทั้งหมดได้เปรียบเสมือนสมุดหน้าเหลือง (Yellow pages) ของข้อมูลภาครัฐ ที่สำคัญทั้งหมดของประเทศไทยซึ่งเป็นจุดเริ่มต้นที่จำเป็นอย่างยิ่งในการพัฒนา การใช้ประโยชน์ข้อมูลภาครัฐให้มีประสิทธิผลและเป็นไปในทิศทางเดียวกันซึ่งจะส่งผลให้สามารถบูรณาการให้บริการและใช้ประโยชน์ข้อมูลข้ามหน่วยงานได้อย่างเป็นระบบ การจัดทำรายการข้อมูลภาครัฐเป็นการรวบรวมคำอธิบายรายการข้อมูลหรือเมทาดาต้า (Metadata) ของข้อมูลสำคัญจากหน่วยงานภาครัฐทั้งหมดมาสร้างเป็นแค็ตตาล็อกเพื่อประโยชน์ในการสืบค้นผ่านระบบสารสนเทศบริการนามานุกรมข้อมูลภาครัฐ (Directory Services) โดยเมทาดาต้าที่รวบรวมจากทุกหน่วยงานควรมีรูปแบบเดียวกันซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจ

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		และสังคม โดยสำนักงานสถิติแห่งชาติจะทำหน้าที่ในการออกแบบกระบวนการและเครื่องมือเพื่อจัดทำมาตรฐานเมทาดาต้าและรวบรวมเมทาดาต้า รายการข้อมูลที่สำคัญจากหน่วยงานรัฐทั้งหมดโดยศึกษาค้นคว้าเปรียบเทียบและวิเคราะห์กรณีศึกษาด้านการจัดทำมาตรฐานเมทาดาต้าของประเทศอื่นเพื่อปรับให้เหมาะสมและเอื้อต่อการแลกเปลี่ยนข้อมูลในประเทศไทยหน่วยงานภาครัฐต่าง ๆ จะสามารถนำมาตรฐานดังกล่าวไปใช้งานและจัดทำเมทาดาต้าของหน่วยงานได้อย่างสอดคล้องกัน กรอบแนวทางการจัดทำรายการข้อมูลภาครัฐ ประกอบด้วย ๑. กำหนดรายละเอียดของชุดข้อมูล (Metadata Template) เช่น ชื่อข้อมูล ผู้รับผิดชอบ วิธีการเก็บ ประเภทข้อมูล รูปแบบข้อมูล เป็นต้น ๒. จัดทำดัชนีสำหรับการสืบค้นข้อมูล (Data Index) สำหรับค้นหาแบบหลายมิติ กำหนดคำสำคัญของข้อมูลกำหนดและจัดกลุ่มข้อมูล เพื่อให้พร้อมสำหรับการสืบค้น โดยดำเนินการร่วมกับหน่วยงานเจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้อง

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		๓. การพัฒนาระบบบริการนามานุกรมข้อมูลภาครัฐ (directory services) เพื่อช่วยให้การสืบค้นผ่านช่องทางต่าง ๆ ทำได้ง่ายขึ้น มีการกำหนดสิทธิ์การเข้าถึงของผู้ใช้ข้อมูลในแต่ละระดับมีกลไกการร้องขอ/อนุมัติข้อมูล และเป็นจุดเชื่อมต่อกับ Data exchange เพื่อการเข้าถึงข้อมูลได้อีกด้วย ๔. การบริการข้อมูล (Data Services) กรณีข้อมูลที่ไม่มีชั้นความลับ open data หรือ public data จะจัดเก็บทั้ง metadata และ data โดยข้อมูลก็ยังคงอยู่ที่เจ้าของข้อมูลเหมือนเดิม เพื่อให้ความสะดวกแก่ผู้ใช้บริการสามารถ download ไปใช้ได้ ส่วนข้อมูลที่เป็นชั้นความลับจะจัดเก็บเฉพาะ metadata เท่านั้น โดยในการเข้าถึงและขอใช้ข้อมูลจะต้องมีกระบวนการร้องขออนุมัติต่อไป ซึ่งขณะนี้ อยู่ระหว่างการจัดเตรียมรายละเอียดเพื่อออกแบบกระบวนการและพัฒนาระบบต่อไป
๙. กระทรวงคมนาคม	**๑. ระบบงานทะเบียนตรวจสภาพรถและภาษีรถยนต์ และรถขนส่ง**	กรมการขนส่งทางบก ได้พัฒนาระบบสารสนเทศที่ใช้ในการจัดเก็บข้อมูลทะเบียนรถซึ่งรถในที่นี้ หมายถึง รถยนต์ รถจักรยานยนต์ รถพ่วง รถบดถนน รถแทรกเตอร์ และรถอื่นตามที่กำหนดในกฎกระทรวง โดยเป็นการดำเนินการ ตาม พ.ร.บ.รถยนต์ พ.ศ. ๒๕๒๒ และ พ.ร.บ.การขนส่งทางบก พ.ศ. ๒๕๒๒ ซึ่งฐานข้อมูล

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		ทะเบียนรถในปัจจุบันได้จัดเก็บข้อมูล ประกอบด้วย เลขทะเบียนรถ เลขตัวรถ เลขเครื่องยนต์ ประเภทรถ ยี่ห้อรถ แบบรุ่น วันที่จดทะเบียน สถานะรถ และสีรถ เป็นต้น สำหรับการเชื่อมโยงข้อมูลนั้น ปัจจุบันได้เชื่อมโยงข้อมูลกับ Linkage Center ของกรมการปกครองแล้ว โดยหน่วยงานภาครัฐสามารถเชื่อมโยงข้อมูลได้
	๒. การจดทะเบียนเรือเพื่อขอรับใบทะเบียนเรือไทย	กรมเจ้าท่าได้พัฒนาระบบสารสนเทศที่ใช้ในการจัดเก็บข้อมูลทะเบียนเรือไทยโดยเป็นการดำเนินการตามพระราชบัญญัติเรือไทย พ.ศ. ๒๔๘๑ ทั้งนี้ ฐานข้อมูลทะเบียนเรือไทยในปัจจุบันได้จัดเก็บข้อมูล อาทิ เลขทะเบียนเรือ ชื่อเรือไทย ชื่อและนามสกุลผู้ควบคุมเรือ วันที่อนุญาตให้ใช้เรือ ความยาวของเรือ ความยาวของฉากเรือ ความกว้างของเรือ ความลึกของเรือ ชื่อผู้ถือกรรมสิทธิ์เรือ หรืออื่น ๆ เป็นต้น สำหรับการเชื่อมโยงข้อมูลนั้น ปัจจุบันได้เชื่อมโยงข้อมูลกับ Linkage Center ของกรมการปกครองแล้ว โดยหน่วยงานภาครัฐสามารถเชื่อมโยงข้อมูลได้ โดยประสานงานกับกรมเจ้าท่า

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
๑๐. สำนักข่าวกรองแห่งชาติ	**โครงการพัฒนาระบบฐานข้อมูลด้านการข่าว**	ศูนย์ประสานข่าวกรองแห่งชาติ (ศป.ข.) ดำเนินการพัฒนาระบบฐานข้อมูลด้านการข่าว โดยในระยะที่ ๑ การเตรียมความพร้อมด้านโครงสร้างพื้นฐาน และการพัฒนาระบบจัดเก็บข้อมูลข่าวสาร ระบบการติดต่อสื่อสารทั้งส่วนกลางและส่วนภูมิภาคด้วยเทคโนโลยีดิจิทัล สำหรับระยะที่ ๒ มีการเชื่อมโยงฐานข้อมูลกับหน่วยสมาชิกในประชาคมข่าวกรองเป็นโครงการนำร่อง และระยะที่ ๓ การเชื่อมโยงฐานข้อมูลกับหน่วยสมาชิกในประชาคมข่าวกรองต่อเนื่องจากระยะที่ ๒ และการพัฒนาระบบวิเคราะห์การนำข้อมูลมาใช้ประโยชน์จัดทำรายงานในรูปแบบต่าง ๆ ตามความต้องการของผู้ใช้ประโยชน์
๑๑. กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์	**๑. ระบบฐานข้อมูลของประเทศไทยด้านการดำเนินคดี และการช่วยเหลือผู้เสียหายจากการค้ามนุษย์**	กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ได้พัฒนาระบบฐานข้อมูลของประเทศไทยด้านการดำเนินคดี และการช่วยเหลือผู้เสียหายจากการค้ามนุษย์ที่ใช้บันทึก จัดเก็บ และเชื่อมโยงข้อมูลคดีค้ามนุษย์ที่เกี่ยวข้องกับหน่วยงานต่างๆ รวมถึงประมวลผลข้อมูลจากระบบฐานข้อมูลเพื่อให้การจัดเก็บและการใช้ข้อมูลเป็นไปในทิศทางเดียวกัน ทั้งในระดับหน่วยงานและภาพรวมของประเทศ เกิดการบูรณาการข้อมูลสารสนเทศระหว่างหน่วยงานที่เกี่ยวข้องอย่างยั่งยืน และสามารถใช้ประโยชน์ในการกำหนดนโยบายด้านการป้องกันและปราบปรามการค้ามนุษย์ของประเทศไทย

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
	๒. ระบบส่งต่อข้อมูลผู้ใช้บริการของกรมกิจการเด็กและเยาวชน (กรมกิจการเด็กและเยาวชน)	ระบบส่งต่อข้อมูลผู้ใช้บริการของกรมกิจการเด็กและเยาวชน เป็นระบบที่จัดเก็บข้อมูลประวัติผู้รับบริการเป็นรายบุคคล (โดยใช้หมายเลขบัตร ๑๓ หลัก) ตาม พ.ร.บ. คุ้มครองเด็ก พ.ศ. ๒๕๔๖ ผู้ถูกกระทำตาม พ.ร.บ. ความรุนแรงในครอบครัว พ.ศ. ๒๕๕๐ และผู้เสียหายตาม พ.ร.บ. ค้ามนุษย์ พ.ศ. ๒๕๕๑ จากบ้านพักเด็กและครอบครัว จำนวน ๗๗ จังหวัด และสถานสงเคราะห์/คุ้มครอง/พัฒนาและฟื้นฟู จำนวน ๓๐ แห่ง ตั้งแต่ข้อมูลการรับแจ้งเรื่องร้องทุกข์ การนำเข้าข้อมูลของผู้ใช้บริการ ข้อมูลครอบครัว ข้อมูลการช่วยเหลือและจัดสวัสดิการ ข้อมูลการส่งต่อหน่วยงานที่เกี่ยวข้องและคืนสู่สังคม ซึ่งปัจจุบันได้ดำเนินการเชื่อมโยงข้อมูลกับกรมการปกครองผ่านระบบ Linkage Center เรียบร้อยแล้ว
	๓. โครงการเปลี่ยนบ้านพักเด็กเป็นสถานคุ้มครองสวัสดิภาพผู้เสียหายจากการค้ามนุษย์(ชาย) ชั่วคราว จำนวน ๒ จังหวัด (กรมกิจการเด็กและเยาวชน)	ดำเนินการเปลี่ยนแปลงหน่วยงานในสังกัดเพื่อเปลี่ยนเป็นสถานคุ้มครองสวัสดิภาพผู้เสียหายจากการค้ามนุษย์(ชาย) ชั่วคราว จำนวน ๒หน่วยงาน ได้แก่ (๑) บ้านพักเด็กและครอบครัวจังหวัดปัตตานี และ (๒) บ้านพักเด็กและครอบครัวจังหวัดพัทลุง ทั้งนี้ ปัจจุบันอยู่ระหว่างการปรับประสิทธิภาพของระบบจัดเก็บฐานข้อมูล
	๔. โครงการส่งเสริมการดำเนินงานตามอนุสัญญาว่าด้วยสิทธิเด็ก (เด็กในบริบทโยกย้ายถิ่นฐาน)	ดำเนินงานเกี่ยวข้องกับการคุ้มครองเด็กในสถานการณ์ จชต. และกำหนดแนวทางและมาตรการทางเลือกในการกักเด็กไว้ในสถานกักตัวคนต่างด้าวของสำนักงานตรวจคน

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		เข้าเมือง สำหรับการเชื่อมโยงฐานข้อมูลนั้น ปัจจุบันอยู่ระหว่างการปรับประสิทธิภาพของระบบจัดเก็บฐานข้อมูล
	๕. โครงการแผ่นดินเดียวกัน	ดำเนินงานเกี่ยวข้องกับการแลกเปลี่ยนวัฒนธรรมของเด็กในพื้นที่สามจังหวัดชายแดนภาคใต้ สำหรับการเชื่อมโยงฐานข้อมูลนั้น ปัจจุบันอยู่ระหว่างการปรับประสิทธิภาพของระบบจัดเก็บฐานข้อมูล
๑๒. กระทรวงการต่างประเทศ (กรมการกงสุล)	**๑. โครงการ Visa Data Center**	พัฒนาระบบการขอรับการตรวจลงตราทางอิเล็กทรอนิกส์ (e-visa) ขึ้นใช้ในการให้บริการในจีน อังกฤษ และฝรั่งเศส เพื่ออำนวยความสะดวกให้แก่คนต่างด้าวและรองรับปริมาณการตรวจลงตราที่เพิ่มมากขึ้น ซึ่งข้อมูลที่ได้รับจากระบบจะถูกส่งมายัง Visa Data Center เพื่อรวบรวมประมวล และแบ่งปันกับหน่วยงานด้านความมั่นคง เช่น สตม. และ สมช. เพื่อประโยชน์ในการติดตามและคัดกรองต่างด้าวที่ต้องการจะเข้าประเทศ ทั้งนี้ กระทรวงฯ จะขยายขอบเขตการให้บริการ e-visa ไปยังประเทศอื่น ๆ ต่อไป
	๒. โครงการ Visa Regional Center	กระทรวงฯ ได้จัดเตรียมงบประมาณเพื่อจัดตั้งศูนย์ฯบริการการตรวจลงตราประจำภูมิภาค (Visa Regional Center) ขึ้น เพื่อรองรับปริมาณการตรวจลงตราผ่านระบบ e-visa ที่จะเพิ่มมากขึ้นในภูมิภาคต่าง ๆ ให้ระบบมีความเสถียรและสามารถลดผลกระทบจากการโจมตีทางไซเบอร์ได้ โดยมีกำหนดจะตั้ง Regional Center ขึ้นที่กรุงปักกิ่ง กรุงนิวเดลี กรุงวอชิงตัน กรุงเบอร์ลิน และกรุงเทพ

หน่วยงาน	ชื่อระบบ/โครงการที่ดำเนินการ	การดำเนินการ
		ทั้งนี้ ในระยะยาว กระทรวงฯ จะมอบหมายให้ Regional Center เหล่านี้เป็นผู้พิจารณาการอนุมัติการตรวจลงตราในภูมิภาคที่กำหนดอีกด้วย

บัญชีอักษรย่อหน่วยงานที่เกี่ยวข้องในตารางการแบ่งมอบหน่วยงาน
แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)
(ภายใต้แนวทางการพัฒนาที่ ๑ - ๔) เรียงตามลำดับอักษร

กค.	กระทรวงการคลัง
กต.	กระทรวงการต่างประเทศ
กษ.	กระทรวงเกษตรและสหกรณ์
กห.	กระทรวงกลาโหม
กอ.รมน.	กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
คค.	กระทรวงคมนาคม
ดศ.	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ตร.	สำนักงานตำรวจแห่งชาติ
พม.	กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
มท.	กระทรวงมหาดไทย
ยธ.	กระทรวงยุติธรรม
รง.	กระทรวงแรงงาน
ศธ.	กระทรวงศึกษาธิการ
ศรชล.	ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล
สขช.	สำนักข่าวกรองแห่งชาติ

สตม.	สำนักงานตรวจคนเข้าเมือง
สธ.	กระทรวงสาธารณสุข
สพร.	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สมช.	สำนักงานสภาความมั่นคงแห่งชาติ
สสช.	สำนักงานสถิติแห่งชาติ
สำนักงาน ก.พ.	สำนักงานคณะกรรมการข้าราชการพลเรือน
สำนักงาน ป.ป.ช.	สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
สำนักงาน ปปง.	สำนักงานป้องกันและปราบปรามการฟอกเงิน

การแบ่งมอบหน่วยงาน
แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

วัตถุประสงค์	ตัวชี้วัด	แนวทางการพัฒนา	หน่วยหลัก	หน่วยประสาน
๑. เพื่อกำหนดกรอบแนวนโยบายการจัดทำฐานข้อมูลด้านความมั่นคง	ระดับความสำเร็จการมีแผนฐานข้อมูลด้านความมั่นคง	**แนวทางการพัฒนาที่ ๑ นโยบายการบูรณาการฐานข้อมูลด้านความมั่นคง** **<u>แนวทางการพัฒนาย่อย</u>** ๑.๑ ศึกษา ทบทวน ปรับปรุงนโยบาย แผน กฎ ระเบียบ ประกาศ คำสั่ง และ แนวทางดำเนินงานของหน่วยงานที่เกี่ยวข้องกับฐานข้อมูลด้านความมั่นคง	สมช. สมช.	กอ.รมน./มท./กห./ยธ./กต./ดศ./ตร. ยธ./สคก.
		๑.๒ เสริมสร้างและบูรณาการข้อมูลร่วมกันเพื่อสนับสนุนยุทธศาสตร์ชาติด้านความมั่นคง แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง การดำเนินนโยบายและแผนงานด้านความมั่นคง	ดศ.	สดช./สพร./กอ.รมน./มท./กห.

<u>หมายเหตุ</u> - หน่วยงานรับผิดชอบหลักสามารถพิจารณากำหนดหน่วยงานสนับสนุนได้ตามความเหมาะสม
- หน่วยงานหลัก เป็นหน่วยงานที่มีหน้าที่โดยตรงนำแนวทางการพัฒนาของแผนการบูรณาการไปสู่การปฏิบัติ
- หน่วยงานสนับสนุน เป็นหน่วยงานที่มีส่วนร่วมและสนับสนุนการดำเนินงานของหน่วยงานหลัก

วัตถุประสงค์	ตัวชี้วัด	แนวทางการพัฒนา	หน่วยหลัก	หน่วยประสาน
		๑.๓ สนับสนุนการมีฐานข้อมูลของหน่วยงานที่สอดคล้องกับสถานการณ์และสภาพปัญหาที่ด้านความมั่นคง	กอ.รมน.	สมช./มท./กห./ยธ./กต./ดศ./ตร./ศรชล.
		๑.๔ กำหนดฐานข้อมูลด้านความมั่นคงในแต่ละประเภทและจัดการลำดับความเร่งด่วนในการจัดเก็บข้อมูล	สมช.	กอ.รมน./มท./กห./ยธ./กต./ดศ./ตร./สตม./ศรชล.
๒. เพื่อพัฒนาระบบข้อมูลในการติดตาม วิเคราะห์ ประเมินสถานการณ์ เพิ่มศักยภาพในการรับมือภัยคุกคาม ป้องกันแก้ไข ระงับ ยับยั้งปัญหาภัยคุกคามและภัยพิบัติ	ระดับความสำเร็จการพัฒนาระบบข้อมูลด้านความมั่นคงระหว่างหน่วยงาน	**แนวทางการพัฒนาที่ ๒ การพัฒนาระบบฐานข้อมูลด้านความมั่นคง** **<u>แนวทางการพัฒนาย่อย</u>** ๒.๑ พัฒนาระบบฐานข้อมูลด้านความมั่นคงทั้งในระดับนโยบายและระดับปฏิบัติที่เหมาะสม	ดศ. ดศ.	สมช./กอ.รมน./สดช./สพร./สสช./สำนักงาน ก.พ. สดช./สพร./สสช./สำนักงาน ก.พ.
		๒.๒ ส่งเสริมและสนับสนุนการจัดทำประเภทบัญชีข้อมูลด้านความมั่นคง (ไม่มีชั้นความลับและกำหนดชั้นความลับ)	กอ.รมน.	กห./สมช./ตร./สดช./สพร./สสช./สำนักงาน ก.พ.

วัตถุประสงค์	ตัวชี้วัด	แนวทางการพัฒนา	หน่วยหลัก	หน่วยประสาน
		๒.๓ ส่งเสริม สนับสนุน พัฒนาเครื่องมือ อุปกรณ์ ระบบเทคโนโลยีที่ทันสมัยให้กับหน่วยงานที่มีหน้าที่ดำเนินการในกิจการงานความมั่นคง	ดศ.	สดช./สพร./สสช.
		๒.๔ พัฒนาและวางแผนโครงสร้างอัตรากำลังและศักยภาพของบุคลากรให้มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้าน	ดศ.	สดช./สพร./สสช./สำนักงาน ก.พ.
๓. เพื่อเพิ่มประสิทธิภาพการแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานด้านความมั่นคงและหน่วยงานที่สนับสนุนภารกิจด้านความมั่นคงให้มีประสิทธิภาพ	ระดับความสำเร็จการมีกลไกการแลกเปลี่ยนเชื่อมโยงข้อมูลระหว่างหน่วยงานด้านความมั่นคง	**แนวทางการพัฒนาที่ ๓ การดำเนินงานด้านเทคนิคเพื่อบูรณาการข้อมูลระหว่างหน่วยงาน**	ดศ.	กอ.รมน./สดช./สพร./สสช./กห./กต./กษ./กค./คค./มท./ยธ./รง./พม./ตร./สธ./ศธ./สขช./สำนักงาน ปปง./สำนักงาน ป.ป.ช.

วัตถุประสงค์	ตัวชี้วัด	แนวทางการพัฒนา	หน่วยหลัก	หน่วยประสาน
		<u>แนวทางการพัฒนาย่อย</u> ๓.๑ พัฒนาโครงสร้างพื้นฐานการจัดเก็บและประมวลผลหน่วยงานที่เกี่ยวข้องที่เหมาะสม มีประสิทธิผลในการใช้งาน	กอ.รมน.	สดช./สพร./สสช./ศรชล.
		๓.๒ พัฒนาระบบสารสนเทศเพื่อบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูล	กอ.รมน.	ดศ./สดช./สพร./สสช.
		๓.๓ พัฒนาระบบรายการข้อมูลภาครัฐ (Government Data Catalog)	กอ.รมน.	ดศ./สดช./สพร./สสช./ศรชล.
		๓.๔ จัดทำระบบวิเคราะห์และจัดทำรายงานให้สอดคล้องกับ Platform ด้านความมั่นคง	ดศ.	ดศ./สดช./สพร./สสช./หน่วยงานที่เกี่ยวข้อง
		๓.๕ สนับสนุนการออกแบบตามกรอบแนวทางที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด	กอ.รมน.	ดศ./สดช./สพร./สสช.

วัตถุประสงค์	ตัวชี้วัด	แนวทางการพัฒนา	หน่วยหลัก	หน่วยประสาน
๔. เพื่อบริหารจัดการข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอที่จะใช้ในการแก้ไขปัญหาความมั่นคงได้อย่างมีประสิทธิภาพ	ระดับความสำเร็จการบริหารจัดการข้อมูลด้านความมั่นคงเพื่อประกอบการเสนอแนะนโยบาย/แผนและแนวทางในการป้องกันและแก้ไขปัญหาความมั่นคง	**แนวทางการพัฒนาที่ ๔ การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง** **<u>แนวทางการพัฒนาย่อย</u>** ๔.๑ การบริหารจัดการแผนบูรณาการข้อมูลด้านความมั่นคงในระดับนโยบาย	สมช. สมช.	กอ.รมน./มท./กห./ศรชล./ตร. กอ.รมน./มท./กห./ศรชล./ตร.
		๔.๒ การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในระดับอำนวยการและประสานการปฏิบัติ	กอ.รมน.	มท./กห./ศรชล./สมช./ตร./ดศ./สดช./สพร./สสช.
		๔.๓ หน่วยงานระดับกระทรวง/กรม ที่เกี่ยวข้องในระดับปฏิบัติสนับสนุนข้อมูลและแลกเปลี่ยนเชื่อมโยงให้กับศูนย์กลางข้อมูลด้านความมั่นคง	กอ.รมน.	สดช./สพร./สสช./หน่วยงานที่เกี่ยวข้อง

วัตถุประสงค์	ตัวชี้วัด	แนวทางการพัฒนา	หน่วยหลัก	หน่วยประสาน
		๔.๔ การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในการรักษาความมั่นคงภายในประเทศ	กอ.รมน	มท./กห./ศรชล./สมช./ตร.
		๔.๕ การอำนวยการและประสานการบูรณาการข้อมูลด้านความมั่นคงในการรักษาความมั่นคงทางทะเล	ศรชล.	กอ.รมน./มท./กห./สมช./ตร./หน่วยงานที่เกี่ยวข้อง
		๔.๖ การจัดทำข้อมูลเพื่อการระดมสรรพกำลัง การกำลังสำรอง และการสัสดี	กห.	หน่วยงานที่เกี่ยวข้อง
		๔.๗ การส่งเสริมความร่วมมือ/ความตกลงเพื่อให้มีการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงาน	สมช.	ดศ./สดช./สพร./สสช. / กอ.รมน./ศรชล./กต.
		๔.๘ การติดตามและประเมินผล	สมช.	กอ.รมน./สพร./ศรชล./มท.

ผนวก จ

บันทึกข้อความ

ส่วนราชการ สำนักงานสภาความมั่นคงแห่งชาติ สถาบันความมั่นคงศึกษา โทร. ๐ ๒๑๔๒ ๐๑๔๒

ที่ นร ๐๘๐๑.๑๓/ ๑๐๐๗๕ **วันที่** ๗๓ ธันวาคม ๒๕๖๒

เรื่อง พิจารณาอนุมัติแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

กราบเรียน นายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ
(ผ่าน รองนายกรัฐมนตรี พลเอก ประวิตร วงษ์สุวรรณ)

๑. **ความเป็นมา**

แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ - ๒๕๘๐) กำหนดให้มีประเด็นการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม โดยให้ความสำคัญกับการบูรณาการข้อมูลด้านความมั่นคง

๒. **การดำเนินงานของ สมช.**

๒.๑ **การจัดทำร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕)** สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ได้จัดทำร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕) มีเป้าหมายเพื่อให้มีระบบฐานข้อมูลและข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้องและสมบูรณ์เพียงพอ สามารถสนับสนุนกลไกการตัดสินใจเพื่อแก้ไขปัญหาความมั่นคงในระดับชาติ พร้อมทั้งกำหนดแนวทางการพัฒนา ๔ แนวทาง คือ ๑) นโยบายการบูรณาการฐานข้อมูลด้านความมั่นคง ๒) การพัฒนาระบบฐานข้อมูลด้านความมั่นคง ๓) การดำเนินงานด้านเทคนิคเพื่อบูรณาการข้อมูลระหว่างหน่วยงาน และ ๔) การบริหารจัดการแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕) โดยมีกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) เป็นหน่วยงานกลาง ทำหน้าที่เป็นศูนย์กลางข้อมูลด้านความมั่นคง (Data Center) **(รายละเอียดร่างแผนฯ ดังแนบท้าย ๑)**

๒.๒ **การพิจารณาร่างแผนฯ** ที่ประชุมคณะกรรมการบูรณาการฐานข้อมูลด้านความมั่นคง ครั้งที่ ๑/๒๕๖๒ เมื่อวันที่ ๒๖ กันยายน ๒๕๖๒ ได้พิจารณาร่างแผนฯ โดยมีรองนายกรัฐมนตรี (พลเอก ประวิตร วงษ์สุวรรณ) เป็นประธาน ที่ประชุมมีมติเห็นชอบร่างแผนฯ และให้นำเสนอสภาความมั่นคงแห่งชาติ โดยมีนายกรัฐมนตรีเป็นประธาน เพื่อพิจารณาความเหมาะสมของร่างแผนฯ ดังกล่าว ทั้งนี้ ได้พิจารณาอนุมัติผลการประชุมแล้ว เมื่อวันที่ ๓ ตุลาคม ๒๕๖๒ **(ผลการประชุมดังแนบท้าย ๒)**

๒.๓ สมช. ได้มีหนังสือสอบถามความเห็นจากสมาชิกสภาความมั่นคงแห่งชาติ โดยได้ให้ความเห็นชอบกับร่างแผนฯ ดังกล่าวแล้ว **(ดังแนบท้าย ๓)**

๓. **ข้อพิจารณา**

๓.๑ ร่างแผนฯ ฉบับนี้ เป็นกรอบทิศทางการบูรณาการข้อมูลความมั่นคงของประเทศ โดยให้ความสำคัญกับการพัฒนาระบบข้อมูลขนาดใหญ่ (Big Data) ด้านความมั่นคง และการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องกับภารกิจความมั่นคงที่สำคัญในด้านต่างๆ ซึ่งจะทำให้เกิดการเชื่อมโยงข้อมูลที่มีความทันสมัยในการป้องกันและแก้ไขปัญหาความมั่นคงมีประสิทธิภาพมากยิ่งขึ้น โดยกำหนดโครงการสำคัญ (Flagship Project) เพื่อรองรับการขับเคลื่อนงานภายใต้แผนฯ ดังกล่าว

๓.๒ ร่างแผนฯ ถือเป็นแผนระดับที่ ๓ ตามแผนแม่บทภายใต้ยุทธศาสตร์ชาติฯ โดยมติที่ประชุมคณะกรรมการยุทธศาสตร์ชาติ ครั้งที่ ๒/๒๕๖๒ เมื่อวันที่ ๒๘ ตุลาคม ๒๕๖๒ เห็นชอบแนวทางการจัดทำแผนระดับที่ ๓ โดยกำหนดชื่อว่า “แผนปฏิบัติการด้าน ... ระยะที่ ... (พ.ศ. ... - ...)” พร้อมทั้งกำหนดระยะเวลาดำเนินงานของแผนให้สอดคล้องกับห้วงเวลาของแผนแม่บทฯ ซึ่งในระยะแรกเป็นการดำเนินการระหว่างปี ๒๕๖๓ - ๒๕๖๕ ดังนั้น สมช. เห็นควรปรับชื่อและระยะเวลาของแผนให้สอดคล้องกับมติคณะกรรมการฯ ดังกล่าว โดยปรับชื่อเป็น **“แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)”**

๔. **ข้อเสนอ**

๔.๑ อนุมัติและประกาศใช้แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

๔.๒ นำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) เสนอที่ประชุมสภาความมั่นคงแห่งชาติ ทราบ

จึงกราบเรียนมาเพื่อกรุณาพิจารณาอนุมัติตามข้อ ๔ หรือสั่งการอื่นใดตามที่เห็นสมควร

พลเอก
(สมศักดิ์ รุ่งสิตา)
เลขาธิการสภาความมั่นคงแห่งชาติ

อนุมัติ
พลเอก
(ประยุทธ์ จันทร์โอชา)
นายกรัฐมนตรี
๙ ธ.ค. ๖๒

กราบเรียน นายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ
เพื่อกรุณาพิจารณาอนุมัติ ในข้อ ๔
พลเอก ประวิตร
รองนายกรัฐมนตรี
๗ ธันวาคม ๒๕๖๒

ที่ กห ๐๑๐๐/๒๐๙๗

กระทรวงกลาโหม
ถนนสนามไชย เขตพระนคร
กรุงเทพมหานคร ๑๐๒๐๐

๒๕ พฤศจิกายน ๒๕๖๒

เรื่อง การร่างแผนบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ - ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๗๙ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามที่ สำนักงานสภาความมั่นคงแห่งชาติ มีหนังสือขอให้พิจารณาความเหมาะสมของร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ - ๒๕๖๕) เพื่อเสนอนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติให้ความเห็นชอบและประกาศใช้แผนฯ ต่อไป นั้น

รัฐมนตรีช่วยว่าการกระทรวงกลาโหม รับทราบแล้ว และเห็นชอบในร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ - ๒๕๖๕)

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

พลเอก
(ชัยชาญ ช้างมงคล)
รัฐมนตรีช่วยว่าการกระทรวงกลาโหม ทำการแทน
รัฐมนตรีว่าการกระทรวงกลาโหม

กองเลขานุการ สำนักรัฐมนตรีฯ
โทร ๐ ๒๒๒๔ ๐๑๑๖
โทรสาร ๐ ๒๒๒๔ ๐๑๑๖

ที่ กค ๐๒๐๒/ ๑๙๓๙๖

กระทรวงการคลัง
ถนนพระราม ๖ กทม. ๑๐๔๐๐

๑๖ ธันวาคม ๒๕๖๒

เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๐ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒ เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

สิ่งที่ส่งมาด้วย สรุปความเห็นเพื่อการแก้ไขและปรับปรุงร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) จำนวน ๒ แผ่น

ตามหนังสือที่อ้างถึง สำนักงานสภาความมั่นคงแห่งชาติขอให้สมาชิกสภาความมั่นคงแห่งชาติพิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) ตามที่สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำร่างฯ แผนดังกล่าวขึ้น ก่อนนำร่างแผนฯ เสนอนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติเพื่อให้ความเห็นชอบและประกาศใช้แผนฯ ต่อไป โดยเมื่อวันที่ ๒๖ กันยายน ๒๕๖๒ ที่ประชุมคณะกรรมการบูรณาการฐานข้อมูลด้านความมั่นคง ครั้งที่ ๑/๒๕๖๒ ซึ่งมีรองนายกรัฐมนตรี (พลเอก ประวิตร วงษ์สุวรรณ) เป็นประธาน ได้มีมติเห็นชอบกับร่างฯ แผนดังกล่าวแล้ว นั้น

กระทรวงการคลัง ขอเรียนว่า เห็นด้วยในหลักการร่างแผนบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) ที่สภาความมั่นคงแห่งชาติจัดทำขึ้น แต่เห็นควรแก้ไข/ปรับปรุงถ้อยคำในร่างแผนฯ ฉบับดังกล่าวรายละเอียดตามสิ่งที่ส่งมาด้วย ทั้งนี้ ในขั้นตอนการนำแผนงาน/โครงการภายใต้ร่างแผนฯ ดังกล่าวไปสู่การปฏิบัติ เห็นควรกำหนดให้มีการจัดทำคำอธิบายข้อมูลของแต่ละชุดข้อมูล (Metadata) อาทิ คำจำกัดความเกี่ยวกับข้อมูล แหล่งที่มาของข้อมูล ลักษณะข้อมูล หน่วยนับ วิธีการเก็บรวบรวมข้อมูล ความถี่ในการรวบรวมข้อมูล และการจัดจำแนกข้อมูล เป็นต้น เพื่อให้ผู้ใช้งานข้อมูลเกิดความเข้าใจถูกต้องตรงกัน ซึ่งจะส่งผลต่อการวิเคราะห์และแปลความหมายข้อมูลได้อย่างถูกต้องต่อไป

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายอุตตม สาวนายน)
รัฐมนตรีว่าการกระทรวงการคลัง

สำนักงานปลัดกระทรวงการคลัง
โทร. ๐ ๒๑๒๖ ๕๙๐๐ ต่อ ๓๒๒๒, ๓๓๐๕
โทรสาร ๐ ๒๒๗๓ ๙๗๙๐

สรุปความเห็นเพื่อการแก้ไขและปรับปรุง
ร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

ประเด็น	เหตุผลสนับสนุน
๑. ร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) หน้า ๒๑	
๑.๑ ตัดข้อความ *"(๓) ระบบ National Single Window (กรมศุลกากร)"* ออก	เนื่องจากระบบ National Single Window เป็นเพียงระบบที่ทำหน้าที่รับ-ส่งข้อมูลภายใต้การรักษาความมั่นคงปลอดภัยทางสารสนเทศและการยืนยันตัวตนของผู้ส่งข้อมูลจากต้นทางไปยังปลายทางเท่านั้น โดยมิได้มีการเก็บข้อมูลของผู้ส่งในลักษณะการนำข้อมูลไปใช้ดำเนินการ หรือประมวล หรืออ้างอิงแต่อย่างใด
๑.๒ แก้ไขข้อความจาก *"(๖) ฐานข้อมูลสินค้าเข้า-ออก สินค้าอันตราย"* เป็น *"(๖) ฐานข้อมูลสินค้าเข้า-ออก และฐานข้อมูลของต้องห้าม-ของต้องกำกัด"*	เนื่องจากสินค้าเข้า-ออกมีมากมายหลากหลายกลุ่ม ประเภทและชนิดขึ้นอยู่กับหลักเกณฑ์การจำแนกกลุ่ม ประเภทและชนิดของสินค้า การวิเคราะห์และตีความข้อมูลเกี่ยวกับสินค้าจึงสามารถกระทำได้หลากหลายมิติ ดังนั้น เพื่อให้การจัดทำแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) ครอบคลุมทุกกลุ่ม ประเภท และชนิดสินค้าที่เกี่ยวข้อง จึงเห็นควรแก้ไขข้อความจาก *"(๖) ฐานข้อมูลสินค้าเข้า-ออก สินค้าอันตราย"* เป็น *"(๖) ฐานข้อมูลสินค้าเข้า-ออก และฐานข้อมูลของต้องห้าม-ของต้องกำกัด"* เนื่องจากได้มีการบัญญัติความหมายของคำทั้งสองคำไว้ในพระราชบัญญัติศุลกากร พ.ศ. ๒๕๖๐ อย่างชัดเจน ดังนี้ • *"ของต้องห้าม"* หมายถึง ของที่มีกฎหมายกำหนดห้ามมิให้นำเข้ามาในหรือส่งออกไปนอกราชอาณาจักร หรือนำผ่านราชอาณาจักร • *"ของต้องกำกัด"* หมายถึง ของที่มีกฎหมายกำหนดว่า หากจะมีการนำเข้ามาในหรือส่งออกไปนอกราชอาณาจักร หรือนำผ่านราชอาณาจักร จะต้องได้รับอนุญาตหรือปฏิบัติให้ครบถ้วนตามที่กำหนดไว้ในกฎหมาย

ประเด็น	เหตุผลสนับสนุน
	อย่างไรก็ดี ภายหลังจากที่มีการประกาศใช้แผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) เรียบร้อยแล้ว เห็นควรมีการประชุมหารือระหว่างหน่วยงานที่เกี่ยวข้องเพื่อกำหนดรายละเอียดของกลุ่ม ประเภทและชนิดสินค้าที่ต้องการให้มีการบูรณาการข้อมูลอีกครั้งหนึ่ง เพื่อให้การใช้งานข้อมูลเกี่ยวกับสินค้าดังกล่าวเกิดประโยชน์และตอบสนองต่อประเด็นการพิจารณาและเป้าหมายที่กำหนดไว้ได้มากที่สุด
๒. ภาคผนวก ก บัญชีข้อมูลด้านความมั่นคงของหน่วยงาน ข้อ ๒. ข้อมูลด้านการบริหารจัดการชายแดน ๒.๓ กระทรวงการคลัง (กรมศุลกากร) หน้า ๑	
๒.๑ ตัดข้อความ *“๑) ระบบ National Single Window”* ออก	โปรดดูเหตุผลในข้อ ๑.๑
๒.๒ แก้ไขข้อความจาก “๒) ฐานข้อมูลสินค้าเข้า-ออก สินค้าอันตราย” เป็น “๒) ฐานข้อมูลสินค้าเข้า-ออก และฐานข้อมูลของต้องห้าม-ของต้องกำกัด”	โปรดดูเหตุผลในข้อ ๑.๒

ด่วนที่สุด

ที่ กต ๐๒๐๐.๕/๑๑๙๕๙

กระทรวงการต่างประเทศ
ถนนศรีอยุธยา กทม. ๑๐๔๐๐

๖ ธันวาคม ๒๕๖๒

เรื่อง การพิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๑ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามหนังสือที่อ้างถึง สำนักงานสภาความมั่นคงแห่งชาติขอให้กระทรวงการต่างประเทศพิจารณาความเหมาะสมของร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) ซึ่งเป็นร่างแผนฯ ที่ได้รับความเห็นชอบจากที่ประชุมคณะกรรมการบูรณาการฐานข้อมูลด้านความมั่นคง ครั้งที่ ๑/๒๕๖๒ เมื่อวันที่ ๒๖ กันยายน ๒๕๖๒ ความละเอียดแจ้งแล้ว นั้น

ขอเรียนว่า หน่วยงานที่เกี่ยวข้องภายในกระทรวงการต่างประเทศได้ร่วมกันพิจารณาร่างแผนฯ แล้ว เห็นว่าเอกสารดังกล่าวมีความเหมาะสมดีแล้ว จึงไม่มีข้อขัดข้องหรือข้อแก้ไขใด ๆ ต่อร่างแผนฯ

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายดอน ปรมัตถ์วินัย)
รัฐมนตรีว่าการกระทรวงการต่างประเทศ

สำนักงานปลัดกระทรวง
กลุ่มงานความมั่นคงระหว่างประเทศ
โทร. ๐ ๒๒๐๓ ๕๐๐๐ ต่อ ๑๒๓๕๔
โทรสาร ๐ ๒๖๔๐ ๔๐๒๓

ด่วนที่สุด

ที่ คค ๐๑๐๐/ ๒๐๘๔ กระทรวงคมนาคม สมศ.
ถนนราชดำเนินนอก กทม.๑๐๑๐๐

๖ พฤศจิกายน ๒๕๖๒

เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๒ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามหนังสือที่อ้างถึง สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) รองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ – ๒๕๘๐) เพื่อให้มีระบบฐานข้อมูลและข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอสามารถสนับสนุนกลไกการตัดสินใจเพื่อแก้ไขปัญหาความมั่นคงในระดับชาติ โดยเมื่อวันที่ ๒๖ กันยายน ๒๕๖๒ ที่ประชุมคณะกรรมการบูรณาการฐานข้อมูลด้านความมั่นคง ครั้งที่ ๑/๒๕๖๒ โดยมีรองนายกรัฐมนตรี (พลเอก ประวิตร วงษ์สุวรรณ) เป็นประธาน มีมติเห็นชอบกับร่างแผนฯ ดังกล่าวแล้ว ความละเอียดแจ้งแล้ว นั้น

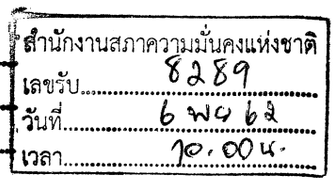
กระผมในฐานะสมาชิกสภาความมั่นคงแห่งชาติ พิจารณาแล้ว เห็นชอบกับร่างแผนบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) ดังกล่าว

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายศักดิ์สยาม ชิดชอบ)
รัฐมนตรีว่าการกระทรวงคมนาคม

สำนักงานรัฐมนตรี
โทร.๐ ๒๒๘๓ ๓๐๑๗
โทรสาร ๐ ๒๒๘๐ ๔๓๐๔



ที่ ดศ ๐๑๐๐.๓.๑๒/๑๐๕๑๗

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
๑๒๐ หมู่ที่ ๓ ศูนย์ราชการเฉลิมพระเกียรติฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐

สมศ.

๓๑ ตุลาคม ๒๕๖๒

เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง พ.ศ. ๒๕๖๒ - ๒๕๖๕

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๓ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามหนังสือที่อ้างถึง สำนักงานสภาความมั่นคงแห่งชาติจัดทำร่างแผนการบูรณาการข้อมูลด้านความมั่นคง พ.ศ. ๒๕๖๒ – ๒๕๖๕ เพื่อรองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑ – ๒๕๘๐) และขอให้สมาชิกสภาความมั่นคงแห่งชาติพิจารณาความเหมาะสมของร่างแผนฯ ก่อนนำร่างแผนฯ ดังกล่าว เสนอนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติให้ความเห็นชอบและประกาศใช้ต่อไป นั้น

ในการนี้ กระผมในฐานะสมาชิกสภาความมั่นคงแห่งชาติพิจารณาแล้วเห็นชอบร่างแผนการบูรณาการข้อมูลด้านความมั่นคง พ.ศ. ๒๕๖๒ – ๒๕๖๕ ตามที่ได้เสนอมา

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

(นายพุทธิพงษ์ ปุณณกันต์)
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานรัฐมนตรี
กลุ่มงานสนับสนุนวิชาการ
โทร. ๐ ๒๑๔๑ ๖๖๐๔
โทรสาร ๐ ๒๑๔๓ ๘๐๐๔

ด่วนที่สุด

ที่ มท ๐๒๑๑.๔/๑๙๓๑๖

กระทรวงมหาดไทย
ถนนอัษฎางค์ กทม. ๑๐๒๐๐

๑๙ พฤศจิกายน ๒๕๖๒

เรื่อง แจ้งผลการพิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๔ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามที่ สำนักงานสภาความมั่นคงแห่งชาติ แจ้งว่า ที่ประชุมคณะกรรมการบูรณาการฐานข้อมูลด้านความมั่นคง ครั้งที่ ๑/๒๕๖๒ เมื่อวันที่ ๒๖ กันยายน ๒๕๖๒ ได้มีมติเห็นชอบร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕) และขอให้รัฐมนตรีว่าการกระทรวงมหาดไทย ในฐานะสมาชิกสภาความมั่นคงแห่งชาติ พิจารณาความเหมาะสมของร่างแผนฯ ดังกล่าว ก่อนนำเสนอนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ เพื่อให้ความเห็นชอบและประกาศใช้แผนฯ ต่อไป ความละเอียดแจ้งแล้ว นั้น

กระทรวงมหาดไทยได้พิจารณาแล้วเห็นว่า ร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕) ดังกล่าวข้างต้น มีความเหมาะสม ครบถ้วน

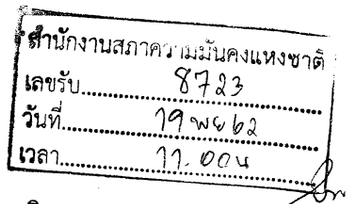
จึงเรียนมาเพื่อทราบ

ขอแสดงความนับถือ

พลเอก
(อนุพงษ์ เผ่าจินดา)
รัฐมนตรีว่าการกระทรวงมหาดไทย

สำนักงานปลัดกระทรวง
สำนักนโยบายและแผน
โทร ๐ ๒๒๒๕ ๓๓๓๙

รับที่ 1025
วันที่ 20 พ.ย. 62
เวลา 9.40 น.



สมศ.

ด่วนที่สุด

ที่ ยธ ๐๒๐๐๘.๕/ ๕๑๑๖

กระทรวงยุติธรรม
ศูนย์ราชการเฉลิมพระเกียรติฯ
อาคารราชบุรีดิเรกฤทธิ์ ชั้น ๙
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐

๑๔ พฤศจิกายน ๒๕๖๒

เรื่อง ความเห็นต่อร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๕ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามหนังสือที่อ้างถึง สำนักงานสภาความมั่นคงแห่งชาติ ขอให้รัฐมนตรีว่าการกระทรวงยุติธรรม ในฐานะสมาชิกสภาความมั่นคงพิจารณาความเหมาะสมของร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) นั้น

ในการนี้ กระทรวงยุติธรรม มีความเห็นว่า ร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ – ๒๕๖๕) ดังกล่าว มีความสอดคล้องกับแผนทั้ง ๓ ระดับ และเป็นประโยชน์ในการนำไปใช้เป็นเครื่องมือกำหนดกรอบแนวนโยบาย การบริหารจัดการ และการจัดทำฐานข้อมูลด้านความมั่นคง เพื่อใช้ในการประเมินสถานการณ์ เตรียมความพร้อมในการรับมือกับภัยคุกคามในด้านต่างๆ และสามารถสนับสนุนกลไกการตัดสินใจเพื่อแก้ไขปัญหาความมั่นคงในระดับชาติได้ ทั้งนี้ หน่วยงานในสังกัดกระทรวงยุติธรรมได้ปรับปรุงข้อมูลในระบบฐานข้อมูลภายใต้โครงการสำคัญตามร่างแผนฯ ที่เกี่ยวข้อง ให้เป็นปัจจุบัน เพื่อรองรับสำหรับการเชื่อมโยงข้อมูลตามแผนฯ ด้วยแล้ว

จึงเรียนมาเพื่อทราบ

ขอแสดงความนับถือ

(นายสมศักดิ์ เทพสุทิน)
รัฐมนตรีว่าการกระทรวงยุติธรรม

สำนักงานปลัดกระทรวงยุติธรรม
กองยุทธศาสตร์และแผนงาน
โทร. ๐ ๒๑๔๑ ๕๓๒๘ (นายทวีพงษ์ แก่นพินิจ)
โทรสาร. ๐ ๒๑๔๓ ๘๒๘๖
E-mail : south_moj@moj.go.th

ด่วนมาก

ที่ กห ๐๓๐๔/ ๕๓๕๖

กรมยุทธการทหาร
กองบัญชาการกองทัพไทย
๑๒๗ ถนนแจ้งวัฒนะ
เขตหลักสี่ กทม. ๑๐๒๑๐

๑๑ ธันวาคม ๒๕๖๒

เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ - ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ/สมาชิกและเลขานุการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๖ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

สำนักงานสภาความมั่นคงแห่งชาติ ขอให้กองบัญชาการกองทัพไทยพิจารณาความเหมาะสมของร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ - ๒๕๖๕) รองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง (พ.ศ.๒๕๖๑ - ๒๕๘๐) รายละเอียดตามอ้างถึง

ผู้บัญชาการทหารสูงสุด/สมาชิกสภาความมั่นคงแห่งชาติ ได้กรุณาพิจารณาแล้วมีความเห็นชอบกับร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ - ๒๕๖๕)

จึงเรียนมาเพื่อกรุณาทราบ

ขอแสดงความนับถือ

พลโท

(ธิติชัย เทียนทอง)
เจ้ากรมยุทธการทหาร

สำนักนโยบายและแผน
โทร. ๐ ๒๕๗๒ ๑๓๑๗

ด่วนมาก
ที่ นร ๕๑๐๐/๖๕๘

กอ.รมน.
สวนรื่นฤดี เขตดุสิต
กรุงเทพมหานคร
๑๐๓๐๐

ธันวาคม ๒๕๖๒

เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๓-๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือ สำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๘ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามที่ สำนักงานสภาความมั่นคงแห่งชาติ ได้จัดทำร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๓-๒๕๖๕) รองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ. ๒๕๖๑-๒๕๘๐) เพื่อให้มีระบบฐานข้อมูลและข้อมูลด้านความมั่นคงที่ทันสมัย ถูกต้อง และสมบูรณ์เพียงพอ สามารถสนับสนุนกลไกการตัดสินใจเพื่อแก้ไขปัญหาความมั่นคงในระดับชาติ โดยขอให้ กอ.รมน. ได้พิจารณาความเหมาะสมของร่างแผนฯ ก่อนนำเสนอ นายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ เพื่อให้ความเห็นชอบและประกาศใช้แผนฯ ต่อไป

กอ.รมน. ตรวจสอบแล้ว ร่างแผนฯ ดังกล่าว มีความเหมาะสม สอดคล้องกับแนวทางการดำเนินการของ กอ.รมน. เพื่อรองรับยุทธศาสตร์ชาติ และแนวทางการพัฒนาข้อมูลขนาดใหญ่ด้านความมั่นคงของ กอ.รมน. เว้นการเป็นเจ้าภาพหลักในเรื่องโครงการบูรณาการข้อมูลด้านปัญหาผู้หลบหนีเข้าเมือง ซึ่ง กอ.รมน. ได้รับมอบหมายเป็นหน่วยงานหลักที่เกี่ยวข้องในเรื่องโครงการ/ระบบ/ข้อมูล แต่เมื่อพิจารณาหน้าที่และอำนาจของหน่วยงานแล้ว สำนักงานตำรวจแห่งชาติ (สำนักงานตรวจคนเข้าเมือง) น่าจะมีความเหมาะสมเป็นเจ้าภาพหลักในการดำเนินการ โดย กอ.รมน. จะเป็นหน่วยร่วมบูรณาการข้อมูล

จึงเรียนมาเพื่อกรุณาพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

พลเอก
(ธีรวัฒน์ บุณยะวัฒน์)
เลขาธิการ กอ.รมน. ปฏิบัติราชการแทน
ผอ.รมน.

สำนักนโยบายและยุทธศาสตร์ความมั่นคง
โทร./โทรสาร. ๐ ๒๒๔๑ ๒๓๔๙

ด่วนมาก

ที่ นร ๕๔๐๐/ ๓๔

ศูนย์อำนวยการรักษาผลประโยชน์
ของชาติทางทะเล ถนนอรุณอมรินทร์
บางกอกน้อย กรุงเทพฯ ๑๐๗๐๐

๔ พฤศจิกายน ๒๕๖๒

เรื่อง ข้อคิดเห็นต่อร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ – ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๔๒๔๙ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามที่ สำนักงานสภาความมั่นคงแห่งชาติ ขอให้ศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) พิจารณาความเหมาะสมร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ – ๒๕๖๗) รองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ.๒๕๖๑ – ๒๕๘๐) ก่อนนำเสนอนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ ให้ความเห็นชอบและประกาศใช้ ตามความแจ้งแล้วนั้น

ศรชล.พิจารณาแล้วเห็นว่า ร่างแผนการบูรณาการข้อมูลด้านความมั่นคงฯ ดังกล่าว จักสนับสนุนการบูรณาการในการปฏิบัติงานร่วมกันระหว่างหน่วยงานรัฐที่เกี่ยวข้องเพื่อเฝ้าระวัง ตรวจสอบหรือเตรียมการป้องกันเพื่อไม่ให้เกิดเหตุการณ์ หรือสถานการณ์ใด ๆ ที่กระทบหรืออาจส่งผลกระทบต่อผลประโยชน์ของชาติทางทะเลหรือกิจกรรมทางทะเล ซึ่งเป็นหน้าที่ของ ศรชล. ตามมาตรา ๒๘ (๒) แห่งพระราชบัญญัติการรักษาผลประโยชน์ของชาติทางทะเล พ.ศ.๒๕๖๒ จึงมีความเหมาะสม

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

พลเรือเอก
(สีทธิพร มาศเกษม)
เลขาธิการศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล ปฏิบัติราชการแทน
ผู้อำนวยการศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล

สำนักนโยบายและแผนความมั่นคงทางทะเล
โทร. ๐ ๒๔๗๕ ๘๕๓๐
โทรสาร ๐ ๒๔๗๕ ๘๕๓๐

สมศ.สมช.
รับที่ 989
วันที่ 17 พ.ย. 62
เวลา 10.00

สำนักงานสภาความมั่นคงแห่งชาติ
เลขรับ 8476
วันที่ 8 พ.ย. 62
เวลา 14.30 น.

ที่ นร ๐๖๑๖/๘๖๗

สำนักข่าวกรองแห่งชาติ
๓๒๑ ถนนราชดำเนินนอก
เขตดุสิต กรุงเทพฯ ๑๐๓๐๐

สมช.

๗ พฤศจิกายน ๒๕๖๒

เรื่อง ความเห็นต่อร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๙๐
ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามหนังสือที่อ้างถึงสำนักงานสภาความมั่นคงแห่งชาติ ขอให้สำนักข่าวกรองแห่งชาติเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของสภาความมั่นคงแห่งชาติ เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕)

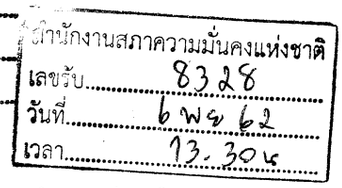
สำนักข่าวกรองแห่งชาติ พิจารณาแล้วเห็นด้วยในหลักการและเหตุผลประกอบร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ. ๒๕๖๒ - ๒๕๖๕) ตามที่สำนักงานสภาความมั่นคงแห่งชาติได้จัดทำขึ้น เพื่อเป็นการบูรณาการข้อมูลด้านความมั่นคงให้เกิดประโยชน์สูงสุดในทุกหน่วยงาน ตอบสนองต่อการดำเนินงานตามแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง บริหารจัดการข้อมูลให้ทันสมัย ถูกต้องและสมบูรณ์ ตลอดจนแก้ไขปัญหาด้านความมั่นคงได้อย่างมีประสิทธิภาพในทุกมิติ

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายอนุกูล เจิมมงคล)
ผู้อำนวยการสำนักข่าวกรองแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐๒ ๒๘๑ ๗๓๙๙ ต่อ ๔๕๓



ที่ ตช ๐๐๐๗.๓๓/๓๕๘๙

สำนักงานตำรวจแห่งชาติ
ถนนพระรามที่ ๑ เขตปทุมวัน
กรุงเทพมหานคร ๑๐๓๓๐

๙ พฤศจิกายน ๒๕๖๒

เรื่อง พิจารณาร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ – ๒๕๖๕)

เรียน เลขาธิการสภาความมั่นคงแห่งชาติ

อ้างถึง หนังสือสำนักงานสภาความมั่นคงแห่งชาติ ที่ นร ๐๘๐๑.๑๓/๘๒๘๗ ลงวันที่ ๑๘ ตุลาคม ๒๕๖๒

ตามหนังสือที่อ้างถึง ขอให้สำนักงานตำรวจแห่งชาติพิจารณาความเหมาะสมของร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ – ๒๕๖๕) รองรับแผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง (พ.ศ.๒๕๖๑ – ๒๕๘๐) ในประเด็นที่เกี่ยวข้อง ความแจ้งแล้ว นั้น

สำนักงานตำรวจแห่งชาติ พิจารณาแล้วเห็นว่าร่างแผนการบูรณาการข้อมูลด้านความมั่นคง (พ.ศ.๒๕๖๒ – ๒๕๖๕) มีความเหมาะสม

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

พลตำรวจโท

(พงษ์วุฒิ พงษ์ศรี)
ผู้ช่วยผู้บัญชาการตำรวจแห่งชาติ ปฏิบัติราชการแทน
ผู้บัญชาการตำรวจแห่งชาติ

สำนักงานยุทธศาสตร์ตำรวจ
โทร. ๐ ๒๒๐๕ ๓๒๘๒
โทรสาร ๐ ๒๒๕๑ ๔๒๔๐

แผนปฏิบัติการ
ด้านการบูรณาการข้อมูลด้านความมั่นคง
ระยะที่ 1 (พ.ศ. 2563-2565)

สถาบันความมั่นคงศึกษา
สำนักงานสภาความมั่นคงแห่งชาติ

เลขที่ 1 ทำเนียบรัฐบาล ถนนพิษณุโลก เขตดุสิต กรุงเทพ 10300
โทรศัพท์ 0-2629-8000 โทรสาร 0-2629-8056
http://www.nsc.go.th/