



# ข้อแนะนำสำหรับการดำเนินการติดตั้งและพัฒนาระบบสารสนเทศ เพื่อสนับสนุนการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

## หลักการและเหตุผล

ตามความในมาตรา ๔ วรรคหนึ่ง แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ และมาตรา ๒๐/๑ วรรคสอง แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๔๒ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ ๓) พ.ศ. ๒๕๕๒ อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา ๒๙ ประกอบกับมาตรา ๓๓ มาตรา ๓๕ มาตรา ๓๖ มาตรา ๔๑ และมาตรา ๔๓ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย กำหนดให้สถาบันการเงินและ ผู้ประกอบอาชีพตามมาตรา ๑๖ จะต้องตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า และระบุตัวตนของลูกค้า โดยสถาบันการเงินและผู้ประกอบอาชีพตามมาตรา ๑๖ (๑) และ (๙) จะต้องกำหนดนโยบายการรับลูกค้าและนโยบายการบริหารความเสี่ยงเกี่ยวกับการฟอกเงินของลูกค้าเป็นลายลักษณ์อักษร

และเมื่อสถาบันการเงินและ ผู้ประกอบอาชีพตามมาตรา ๑๖ ได้ดำเนินการระบุตัวตนของลูกค้าแล้วเสร็จ ก็จะต้องดำเนินการตามกระบวนการในการบริหารความเสี่ยง โดยจะต้องมีการจัดระดับความเสี่ยงต่อการฟอกเงินของลูกค้า โดยการตรวจสอบลูกค้ากับฐานข้อมูลต่างๆที่เกี่ยวกับ ประเทศหรือพื้นที่ที่ลูกค้ามีถิ่นที่อยู่ แหล่งรายได้ การประกอบอาชีพ หรือความเป็นบุคคลที่มีสถานภาพทางการเมืองในต่างประเทศ

ดังนั้น เพื่อให้การปฏิบัติตามกฎหมายในการตรวจสอบลูกค้ากับฐานข้อมูลต่างๆ มีความปลอดภัย มีความน่าเชื่อถือในการรายงานธุรกรรม และมีการจัดการข้อมูลเป็นมาตรฐานเดียวกัน ทางสำนักงาน ปปง. จึงได้ออกข้อแนะนำสำหรับผู้ให้บริการเพื่อมาดำเนินการในการพัฒนาและให้บริการเพื่อสนับสนุนการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า ซึ่งต้องมีคุณสมบัติในด้านต่างๆ และดำเนินงานตามขั้นตอนดังต่อไปนี้



# คุณสมบัติและขั้นตอนการดำเนินการของผู้ให้บริการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (CDD Gateway)

## คุณสมบัติของผู้ให้บริการ CDD Gateway

๑. เป็นบริษัทจำกัด หรือบริษัทจำกัด (มหาชน) มีทุนจดทะเบียนไม่น้อยกว่า ๕๐ ล้านบาท หรือหน่วยงานราชการ
๒. ไม่ประกอบธุรกิจที่มีความเสี่ยง ที่เป็นสาเหตุของของความเสียหายต่อสาธารณะ หรือความมั่นคงทางการเงินของประเทศ (Causing damage to public or financial stability)
๓. กรรมการ/ผู้มีอำนาจจัดการไม่มีลักษณะต้องห้าม เช่น ถูกพิทักษ์ทรัพย์, (เคย) ล้มละลาย และยังไม่พ้น ๒ ปี นับแต่ยกเลิกหรือปลดจากการล้มละลาย หรือเคยได้รับโทษจำคุกในคดีอาญาซึ่งศาลได้มีคำพิพากษาถึงที่สุด
๔. มีประสบการณ์ในการให้บริการพัฒนาระบบสารสนเทศที่เกี่ยวข้องกับการรับส่งข้อมูล หรือเป็นผู้ให้บริการระบบคอมพิวเตอร์ในการรับส่งข้อมูล
๕. ใช้ระบบคอมพิวเตอร์ฮาร์ดแวร์และซอฟต์แวร์ที่ถูกจัดลำดับความน่าเชื่อถือตามหลักมาตรฐานความมั่นคงปลอดภัยเป็นที่ยอมรับในระดับสากล
๖. ผู้ให้บริการต้องจัดให้มีการดำเนินงานพร้อมทั้งมีบุคลากรที่มีความเชี่ยวชาญเฉพาะในการบริหารจัดการตามหลักมาตรฐานความมั่นคงปลอดภัยในระบบสารสนเทศ (Information Security Management System) โดยต้องได้รับการรับรองมาตรฐาน ISO/IEC 27001:2005 จากหน่วยงานผู้ออกใบรับรองที่มีความน่าเชื่อถือในระดับสากล

## คุณลักษณะของระบบ CDD Gateway

ระบบ CDD Gateway ควรมีคุณลักษณะดังต่อไปนี้

๑. ต้องมีระบบตรวจสอบกลับกรอง (Filtering) ระหว่างข้อมูลลูกค้า กับข้อมูลบัญชีรายชื่อเฝ้าระวัง (Watchlist) โดยสำนักงาน ปปง. เป็นผู้กำหนด เพื่อให้บริการแก่ผู้ที่มีหน้าที่รายงานธุรกรรม และรายงานผลการตรวจสอบกลับไปยังผู้ใช้บริการ โดยสามารถให้บริการได้ ๓ รูปแบบดังนี้
  - ๑.๑. การตรวจสอบแบบออนไลน์สำหรับผู้ใช้งาน (End User Online Processing) สามารถใช้งานผ่านระบบ Web Application โดยใช้ Web Browser ที่เครื่องคอมพิวเตอร์ของผู้ใช้งาน (Workstation) โดยสามารถตรวจสอบได้ครั้งละ ๑ รายชื่อ
  - ๑.๒. การตรวจสอบแบบออนไลน์ โดยใช้เว็บเซอร์วิส (Web Services Online Processing) เพื่อให้บริการในรูปแบบการเชื่อมต่อโดยตรงระหว่างระบบ CDD Gateway และระบบคอมพิวเตอร์แม่ข่ายของผู้ให้บริการ (Host-to-Host Communication) โดยสามารถตรวจสอบได้ ๑ รายชื่อ ต่อการเรียกใช้ Web Service ในแต่ละครั้ง
  - ๑.๓. การตรวจสอบแบบแบทช์ (Batch Processing) เป็นการเชื่อมต่อโดยตรงระหว่างระบบคอมพิวเตอร์แม่ข่าย (Computer Server) ของผู้ให้บริการ โดยผ่านระบบ Messaging Gateway ของผู้ให้บริการ CDD Gateway เพื่อให้ผู้ใช้บริการทำการตรวจสอบรายชื่อของลูกค้าจำนวนหลายรายการได้พร้อมกันระบบต้องสามารถรองรับข้อมูลการวิเคราะห์ความเสี่ยงของรายงานธุรกรรม ที่มีเหตุอันควรสงสัยว่าเกี่ยวข้องกับการฟอกเงินหรือการสนับสนุนทางการเงินแก่การก่อการร้าย ภายใต้กฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน
๒. มีระบบวิเคราะห์ความเสี่ยง (Risk Analysis) เพื่อสนับสนุนการวิเคราะห์และจัดระดับความเสี่ยงในการทำธุรกรรมที่มีเหตุอันควรสงสัย
๓. ต้องสามารถใช้งานกับข้อมูลบัญชีรายชื่อบุคคลที่ต้องจับตาเฝ้าระวัง (Watchlist) ได้หลากหลาย เช่น UN, EU, OFAC, BOE, ฐานข้อมูลเชิงพาณิชย์ รวมถึงข้อมูลที่สำนักงาน ปปง. กำหนด เป็นต้น
๔. มีระบบรองรับสำหรับจัดเตรียมและเชื่อมโยงข้อมูล กับผู้ให้บริการข้อมูลบัญชีรายชื่อบุคคลที่ต้องจับตาเฝ้าระวัง (Watchlist) ในข้อ ๓ โดยมีคุณสมบัติดังนี้
  - ๔.๑. สามารถทำการรวบรวมข้อมูลบัญชีรายชื่อบุคคลที่ต้องจับตาเฝ้าระวังจากข้อมูลที่เกี่ยวข้อง
  - ๔.๒. มีระบบในการเพิ่มรายชื่อ ประเภทของรายชื่อ และข้อมูลที่เกี่ยวข้องทั้งหมด โดยใช้งานผ่านทาง Web Browser

- ๔.๓. มีระบบในการร้องขอข้อมูลทั้งหมด (Fully Update) และข้อมูลที่ปรับปรุง (Incremental Update) โดยสามารถระบุช่วงเวลาในการร้องขอได้
๕. ระบบคอมพิวเตอร์ฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และอุปกรณ์อื่นๆ ของผู้ให้บริการต้องทำการเชื่อมต่อกับฐานข้อมูลบัญชีรายชื่อบุคคลที่ต้องจับตาเฝ้าระวัง (Watchlist Database) ณ ศูนย์ข้อมูลหลักของสำนักงาน ป.ป.ง. หรือตามที่สำนักงาน ป.ป.ง.เป็นผู้กำหนดสถานที่ โดยเจ้าหน้าที่ของสำนักงาน ป.ป.ง. เป็นผู้รับผิดชอบดูแลและจัดการระบบฐานข้อมูล
๖. ต้องมีระบบการรับส่งข้อมูลโดยใช้รูปแบบของ XML File Format เพื่อรองรับข้อมูล (รายชื่อที่ต้องการตรวจสอบ) และข้อมูลรายการธุรกรรมทางการเงิน ของผู้ที่มีหน้าที่รายงานธุรกรรมที่มีเหตุอันควรสงสัยว่าเกี่ยวข้องกับฟอกเงินหรือการสนับสนุนทางการเงินแก่การก่อการร้าย แบบแบตช์ (Batch) ในการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า
๗. ต้องมีระบบซอฟต์แวร์สำหรับจัดเตรียมและเชื่อมโยงข้อมูล เพื่อติดตั้งที่สำนักงาน ป.ป.ง. หรือของสถาบันการเงิน หรือผู้ที่มีหน้าที่รายงานธุรกรรมที่มีเหตุอันควรสงสัยว่าเกี่ยวข้องกับฟอกเงินหรือการสนับสนุนทางการเงินแก่การก่อการร้าย ตามที่สำนักงาน ป.ป.ง. เป็นผู้กำหนด โดยมีคุณสมบัติดังนี้
- ๗.๑. มีระบบในการแปลงรูปแบบของไฟล์ข้อมูล (Data Format Transformation) ให้อยู่ในรูปแบบ XML ตามโครงสร้างข้อมูล (XML Schema) หรือให้อยู่ในรูปแบบไฟล์ข้อมูลรูปแบบอื่นๆ ตามที่สำนักงาน ป.ป.ง. กำหนด
- ๗.๒. มีระบบในการเชื่อมโยงเพื่อรับ-ส่งข้อมูลกับระบบ CDD Gateway โดยมีคุณสมบัติตรงตามข้อกำหนดในข้อ ๑๑
๘. รองรับการยืนยันตัวตนบุคคลด้วยลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature) รวมถึงการเข้ารหัส/ถอดรหัส (Encrypt/Decrypt)
๙. ระบบต้องสนับสนุนการทำงานร่วมกับ Public Key Infrastructure (PKI) ได้แก่ RSA, 3DES, DES, AES, SHA, X.509, PKCS, CRLs หรือ OCSP และ XML Signature
๑๐. ระบบต้องมีการบันทึกประวัติ เวลาการเข้าใช้งานระบบ และการดำเนินการตรวจสอบข้อมูลในแต่ละครั้ง รวมถึงข้อมูลที่จำเป็นต่างๆ (Activity Logging) ในรูปแบบ log file

๑๑. ต้องมีระบบในการเชื่อมโยงข้อมูล ซึ่งมีคุณสมบัติดังนี้

- ๑๑.๑. ระบบต้องสามารถตรวจสอบหรือมีกระบวนการ ในการยืนยันตัวตนได้ว่าผู้ที่ร้องขอข้อมูลเข้ามานั้น มีสิทธิในการเข้าถึงข้อมูลที่ต้องการได้
  - ๑๑.๒. ระบบต้องสนับสนุนโครงสร้างการทำงานแบบ **Service Oriented Architecture (SOA)** หรือรองรับการเชื่อมต่อในรูปแบบ **Web Services**
  - ๑๑.๓. ระบบต้องสนับสนุนการทำงานตามมาตรฐาน **Web Services** ดังต่อไปนี้ **SOAP, Universal Description Discovery and Integration (UDDI), และ Web Services Description Language (WSDL)**
  - ๑๑.๔. ต้องมีระบบที่ใช้งานผ่าน **Web Browser** โดยใช้โปรโตคอล **HTTPS** ในการรับส่งข้อมูล
  - ๑๑.๕. มีระบบ **Message Handler Service** ที่สามารถทำงานร่วมกับโปรโตคอล **HTTP/HTTPS, Web Services** หรือ **ebXML Version 2.0** หรือดีกว่า ได้อย่างมีประสิทธิภาพ
  - ๑๑.๖. รองรับการทำ **XML validation** เพื่อตรวจสอบความถูกต้องของข้อมูล
  - ๑๑.๗. มีระบบ **Automatic Processing Notification** การแสดง **Error Message** แจ้งให้ผู้ใช้ทราบ โดยอัตโนมัติในทันที
  - ๑๑.๘. ต้องมีระบบสืบค้นประวัติการใช้งานระบบ (**Transaction Tracking**) ผ่านเครือข่ายอินเทอร์เน็ตได้อย่างมีประสิทธิภาพ
  - ๑๑.๙. มีระบบการควบคุมเป็นแบบรวมศูนย์ ที่สามารถทำการกำหนดค่า (**Configuring**) ดูแลระบบ (**Administering**) และตรวจสอบการทำงาน (**Monitoring**) ได้
๑๒. ผู้ให้บริการ **CDD Gateway** จะต้องจัดให้มีเจ้าหน้าที่ดูแลระบบ เพื่อดำเนินการตรวจสอบการทำงานของระบบ (**Monitoring**) ให้มีเสถียรภาพอยู่เสมอ เพื่อให้ผู้ใช้สามารถใช้งานระบบได้อย่างต่อเนื่องและมีประสิทธิภาพ
๑๓. เป็นระบบที่ออกแบบและให้บริการ **CDD Gateway** เฉพาะสำหรับ สำนักงาน ปง. โดยเจ้าหน้าที่ดูแลระบบของสำนักงาน ปง. มีสิทธิในการเข้าควบคุมและตรวจสอบตลอดเวลา การเชื่อมต่อเข้ามาในระบบ **CDD Gateway** เพื่อดำเนินการใดๆของเจ้าหน้าที่ของผู้ให้บริการ **CDD Gateway** ไม่ว่าจะเข้ามาโดยผ่านระบบควบคุมของเครื่องคอมพิวเตอร์ หรืออุปกรณ์ใดๆโดยตรง รวมถึงการเชื่อมต่อเข้ามาในระบบผ่านระบบควบคุมระยะไกล (**Remote Access Administration**) จะต้องได้รับอนุญาตจากสำนักงาน ปง. ทุกครั้ง

๑๔. มีระบบ **Production Server** ที่มีการทำ **Fully Redundant** ซึ่งสามารถทำงานทดแทนซึ่งกันและกันได้โดยมีประสิทธิภาพ ในกรณีที่อุปกรณ์ใดอุปกรณ์หนึ่งไม่สามารถใช้งานได้ โดยข้อมูลทั้งสองระบบต้อง **Update** เหมือนกันแบบ **Real-time** หรือระบบ **Backup** อื่นๆที่ดีกว่า เช่น การทำ **Backup Site** หรือ **Disaster Recovery Center (DRC)** เป็นต้น
๑๕. ผู้ให้บริการต้องทำการติดตั้งระบบ **CDD Gateway** ภายในศูนย์ข้อมูล (**Data Center**) ของ ปง. หรือศูนย์ข้อมูลของผู้ให้บริการ (**Data Center Service Provider**) ตามที่สำนักงาน ปง. กำหนด โดยผู้ให้บริการต้องเป็นผู้รับผิดชอบภาระค่าใช้จ่ายในการเช่าใช้บริการ ในกรณีที่ต้องทำการติดตั้งระบบ **CDD Gateway** ภายในศูนย์ข้อมูลของผู้ให้บริการศูนย์ข้อมูลภายนอก
๑๖. ผู้ให้บริการต้องจัดให้มีระบบสำรองสำหรับการให้บริการ **CDD Gateway** ที่มีประสิทธิภาพเท่ากับระบบให้บริการหลัก โดยทำการติดตั้งระบบสำรองภายในศูนย์ข้อมูล (**Data Center**) คนละแห่งกับระบบให้บริการหลัก
๑๗. ผู้ให้บริการต้องจัดให้มีระบบการเชื่อมต่อเครือข่ายอินเทอร์เน็ตด้วยความเร็ว **10Mbps** เป็นอย่างน้อย เพื่อให้บริการแก่หน่วยงานภายนอก ในการใช้บริการ **CDD Gateway**
๑๘. ผู้ให้บริการต้องจัดให้มีระบบการเชื่อมต่อเครือข่ายสื่อสารระยะไกล (**Wide Area Network**) ด้วยความเร็ว **5 Mbps** เป็นอย่างน้อย ระหว่าง ศูนย์ข้อมูลหลัก และ ศูนย์ข้อมูลสำรองของ **CDD Gateway** พร้อมทั้งจัดให้มีระบบซอฟต์แวร์ที่เหมาะสมเพื่อใช้สำหรับเชื่อมโยงข้อมูลกับศูนย์ข้อมูลหลักของสำนักงาน ปง.
๑๙. ผู้ให้บริการจะต้องจัดให้มีระบบการเชื่อมต่อเครือข่ายสื่อสารระยะไกล (**WAN**) ด้วยความเร็ว **2Mbps** เป็นอย่างน้อย เพื่อใช้ในการเชื่อมโยงระบบคอมพิวเตอร์ ระหว่าง
- ๑๙.๑. ศูนย์ข้อมูลหลักของ **CDD Gateway** และ ศูนย์ข้อมูลหลักของ ปง.
  - ๑๙.๒. ศูนย์ข้อมูลหลักของ **CDD Gateway** และ ศูนย์ข้อมูลสำรองของ ปง.
  - ๑๙.๓. ศูนย์ข้อมูลสำรองของ **CDD Gateway** และ ศูนย์ข้อมูลหลักของ ปง.
  - ๑๙.๔. ศูนย์ข้อมูลสำรองของ **CDD Gateway** และ ศูนย์ข้อมูลสำรองของ ปง.
๒๐. ผู้ให้บริการต้องจัดให้มีระบบรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพเหมาะสมในการให้บริการ เช่น **Firewall, Intrusion Prevention System (IPS)** เป็นต้น พร้อมทั้งจัดให้มีการศึกษา วิเคราะห์ ตรวจสอบ ข้อบกพร่อง หรือช่องโหว่ ของระบบฮาร์ดแวร์ ระบบเครือข่าย และระบบซอฟต์แวร์ อย่างสม่ำเสมอ เพื่อปกป้องระบบการให้บริการและข้อมูลที่เป็นความลับของ ปง.

๒๑. ผู้ให้บริการต้องจัดให้มีระบบตรวจสอบและการอนุญาตในการเข้าถึงระบบ **CDD Gateway** ของผู้ให้บริการผ่านระบบเครือข่ายทางไกล ที่มีความปลอดภัย เช่น การใช้เทคโนโลยี **SSL VPN** และ **2-Factor Authentication** เป็นต้น
๒๒. ผู้ให้บริการต้องจัดให้มีแผนสำรองฉุกเฉินในกรณีที่เกิดเหตุภัยพิบัติหรือเหตุการณ์ไม่คาดฝัน (**Disaster Recovery Planning**) ดังนี้
- ๒๒.๑. มีการจัดเตรียมระบบสำรอง โดยจะต้องสามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา โดยติดตั้งอยู่อีกสถานที่หนึ่งมีการเชื่อมต่อเครือข่ายถึงกันและปรับปรุงข้อมูลแบบเรียลไทม์
  - ๒๒.๒. มีกระบวนการประสานงานที่มีการจัดเตรียมไว้แล้ว ในการนำระบบ ข้อมูล และโครงสร้าง (**infrastructure**) ที่จำเป็นกลับคืนมา เพื่อสนับสนุนให้ระบบสามารถดำเนินงานต่อไปได้
  - ๒๒.๓. มีการจัดทำแผนที่รายการละเอียดชัดเจนเพื่อที่จะป้องกัน ในกรณีที่มีการหยุดให้บริการในส่วนของระบบสารสนเทศและข้อมูลที่สำคัญจากผลกระทบของความเสียหายต่างๆ
  - ๒๒.๔. มีการระบุเหตุการณ์ความเสียหาย การวิเคราะห์ผลกระทบต่อระบบ การประเมินความเสี่ยง และการวางแผนนโยบายและแนวทางในการจัดทำแผนสำรองฉุกเฉิน
๒๓. ผู้ให้บริการต้องจัดให้มีการตรวจสอบเพื่อประเมินประสิทธิภาพของระบบ **CDD Gateway** อย่างสม่ำเสมอ พร้อมทั้งจะต้องวางแผนและทำการปรับปรุงเพื่อเพิ่มประสิทธิภาพของระบบ **CDD Gateway** ด้วยงบประมาณของผู้ให้บริการเอง ให้เหมาะสมสอดคล้องกับจำนวนของผู้ใช้บริการ ตลอดจนปริมาณงานและกิจกรรมต่างๆที่อาจเพิ่มขึ้นในอนาคต
- ซึ่งคุณลักษณะของ **CDD Gateway** ที่ทางสำนักงาน ปปง. กำหนดไว้นั้น จะมีการพิจารณาตามสถาปัตยกรรมและเทคโนโลยีที่ผู้ให้บริการเลือกใช้ รวมถึงรูปแบบการรายงานที่ให้บริการ โดยทางสำนักงาน ปปง. จะเป็นผู้พิจารณาจากการนำเสนอของผู้ให้บริการ



## ขั้นตอนในการขอเป็นผู้ให้บริการ CDD Gateway

๑. ผู้ขอให้บริการ CDD Gateway จะต้องนำเสนอเอกสาร Proposal ให้แก่สำนักงาน ปปง. โดยรายละเอียดของเอกสาร Proposal จะต้องประกอบด้วยหัวข้อ ดังต่อไปนี้
  - ๑.๑. รายละเอียดประวัติของบริษัท (Company profile)
  - ๑.๒. ข้อมูลและรายละเอียดเกี่ยวกับประสบการณ์ในการพัฒนาระบบสารสนเทศ (Gateway) ที่เกี่ยวข้องกับ การรับส่งข้อมูล หรือเป็นผู้ให้บริการระบบสารสนเทศในการรับส่งข้อมูล พร้อมทั้งรายชื่อหน่วยงานที่มี การให้บริการอยู่ ณ ปัจจุบัน
  - ๑.๓. เอกสารการจดทะเบียน ได้แก่ หนังสือรับรองการจดทะเบียนบริษัท
  - ๑.๔. เอกสารแสดงคุณสมบัติของบริการ Gateway

ผู้ขอผู้ให้บริการ CDD Gateway จะต้องส่งเอกสาร Proposal ให้กับสำนักงาน ปปง. ภายในวันที่ ๗ สิงหาคม ๒๕๕๕ หากส่งภายหลังจากนี้ทางสำนักงาน ปปง. จะพิจารณาในรอบถัดไป (ซึ่งทางสำนักงาน ปปง. จะทำการ ประกาศวันพิจารณาในรอบถัดไปอีกครั้งหนึ่ง)

๒. ภายหลังจากการนำเสนอ Proposal สำนักงาน ปปง. จะแจ้งให้ผู้ขอให้บริการ CDD Gateway นำเสนอ รายละเอียดของระบบงานและแผนในการดำเนินงาน ให้แก่สำนักงาน ปปง. เพื่อแสดงความรู้ความเข้าใจ เกี่ยวกับระบบงานที่จะให้บริการ โดยจะต้องมีเอกสารประกอบดังนี้
  - ๒.๑. โครงสร้างการทำงานของระบบ
  - ๒.๒. ฟังก์ชันการทำงาน ตลอดจนเอกสารอื่นๆ ที่เกี่ยวข้อง
  - ๒.๓. รายละเอียดของอุปกรณ์และ Server ตลอดจน Software ต่าง ๆ ที่ต้องใช้ในการบริหารจัดการระบบ ทั้ง Primary Site และ Backup Site
  - ๒.๔. งบประมาณในการลงทุนพัฒนาระบบและการดำเนินงาน

โดยต้องส่งเอกสารเหล่านี้ให้แก่สำนักงาน ปปง. ภายในวันที่ ๑๔ สิงหาคม ๒๕๕๕

๓. ภายหลังจากการนำเสนอ Proposal พร้อมรายละเอียดการดำเนินงาน สำนักงาน ปปง. จะแจ้งให้ผู้ขอให้บริการ CDD Gateway กำหนดวันเวลาพร้อมการจัดเตรียมระบบดังกล่าวเพื่อทดสอบเสมือนจริงในการทำงานควบคู่

กับระบบของสำนักงาน ปปง. และระบบของผู้รายงานธุรกรรม โดยจะต้องทำการทดสอบดังกล่าวต่อไปนี้ เป็นอย่างน้อย

๓.๑. **Functional Test**

๓.๒. **System Integration Test**

๓.๓. **Load Test**

สำนักงาน ปปง. จะเรียกผู้ให้บริการ **CDD Gateway** เข้าทดสอบเสมือนจริงในโอกาสแรก ทั้งนี้ระยะเวลาขึ้นอยู่กับลำดับการยื่นเอกสารและความพร้อมของผู้ให้บริการ โดยจะพิจารณาว่าผู้ให้บริการจะสามารถให้บริการได้ภายในช่วงระยะเวลาที่กฎหมายมีผลบังคับใช้เป็นต้นไป

๔. เมื่อผู้ให้บริการ **CDD Gateway** แสดงได้ว่าสามารถให้บริการได้จริง ผู้ให้บริการ **CDD Gateway** ต้องนำเสนอแผนการดำเนินงานของผู้ให้บริการ **CDD Gateway** ก่อนการให้บริการจริง โดยต้องระบุขั้นตอนต่างๆอย่างละเอียด และระบุวันที่สามารถให้บริการได้จริง

๕. ผู้ที่มีคุณสมบัติเหมาะสมในการให้บริการ **CDD Gateway** ต้องสามารถพัฒนาระบบงานและดำเนินการที่เกี่ยวข้องให้สำนักงาน ปปง. ได้โดยไม่คิดค่าใช้จ่ายใดๆกับสำนักงาน ปปง. ทั้งนี้การดำเนินการมีดังต่อไปนี้

๕.๑. การรักษาความลับ

๕.๑.๑. ผู้ให้บริการ **CDD Gateway** ต้องดำเนินการทั้งปวงด้วยความละเอียดรอบคอบ และระมัดระวังเพื่อรักษาความลับของข้อมูลของทุกหน่วยงานที่เกี่ยวข้องกับระบบของสำนักงาน ปปง. และความมั่นคงปลอดภัยของระบบของสำนักงาน ปปง.

๕.๑.๒. ผู้ให้บริการ **CDD Gateway** จะต้องจัดทำแผนปฏิบัติการเกี่ยวกับการทำงานทั้งปวงที่เกี่ยวข้องกับระบบของสำนักงาน ปปง. ที่แสดงให้เห็นถึงการรักษาความลับของข้อมูลและความปลอดภัยของระบบของสำนักงาน ปปง. ที่สามารถตรวจสอบได้

๕.๑.๓. ผู้ให้บริการ **CDD Gateway** ต้องจัดทำขั้นตอนการปฏิบัติงานอย่างละเอียดเกี่ยวกับการเข้าถึง **Gateway** และการปฏิบัติงานใน **Data Center** รวมถึงตรวจสอบการปฏิบัติงานของพนักงานที่เกี่ยวข้องกับระบบ **Gateway**

๕.๑.๔. กรณีเกิดความเสียหายอันมีสาเหตุมาจากการจัดการ และ/หรือการปฏิบัติงานของพนักงานของผู้ให้บริการ **CDD Gateway** ทั้งการเข้า **Data Center** หรือการปฏิบัติงานผ่านระบบเครือข่ายทางไกลในส่วนที่เกี่ยวข้องกับระบบของสำนักงาน

๕.๑.๕. การเข้าถึงสถานที่ติดตั้งระบบของผู้ให้บริการ **CDD Gateway** ต้องปฏิบัติตามระเบียบการเข้าถึง **Data Center** อย่างเคร่งครัด

- ๕.๑.๖. การเข้าถึงระบบของผู้ให้บริการ CDD Gateway ผ่านระบบเครือข่ายทางไกล ต้องดำเนินการด้วยวิธีที่มีความปลอดภัย และต้องปฏิบัติตามกฎระเบียบการเข้าถึงระบบของผู้ให้บริการ Gateway โดยเคร่งครัด
- ๕.๑.๗. การพัฒนาระบบการบันทึกข้อมูลการเข้าถึงระบบ จะต้องจัดเก็บข้อมูลการทำงานทุกกิจกรรม
- ๕.๑.๘. ผู้ให้บริการ CDD Gateway ต้องสามารถปฏิบัติตามกฎหมาย และระเบียบเกี่ยวกับการรักษาความลับของทางราชการได้



## ๕.๒. การให้บริการ Help Desk และ Call Center โดยมีข้อกำหนดในการให้บริการดังนี้

ประเภทบริการ	ข้อกำหนดของการให้บริการ
๑. การให้บริการ Help Desk และ Call Center ของ Gateway	Call Center ต้องสามารถให้บริการได้ทุกวันตลอด ๒๔ ชั่วโมงโดยไม่มีวันหยุด นับตั้งแต่เปิดให้บริการ Gateway
๒. การติดต่อสอบถามเจ้าหน้าที่ Help Desk และ Call Center ทางโทรศัพท์	ผู้ให้บริการ ๕ ครั้ง จะต้องสามารถติดต่อเจ้าหน้าที่ Help Desk และ Call Center ได้อย่างน้อย ๓ ครั้ง (คำนวณค่าเฉลี่ยรายวัน ระหว่างเวลา ๙.๓๐ - ๑๗.๓๐ น.) เว้นแต่เกิดปัญหาอันพิสูจน์ได้ว่าเกิดจากหน่วยงานอื่น เช่น ผู้ให้บริการ
๓. การติดต่อสอบถามเจ้าหน้าที่ Help Desk และ Call Center ทางอีเมลล์	Help Desk และ Call Center ต้องมีความรู้ความสามารถในการตอบคำถามเรื่องของการรายงานธุรกรรมตามกฎหมายการฟอกเงิน ทั้งทางด้านเทคนิคและอื่นๆ
๔. การจัดเก็บข้อมูลการใช้บริการ	มีระบบบันทึกการสนทนาระหว่างเจ้าหน้าที่ Help Desk และ Call Center และผู้ให้บริการ โดยระบบต้องแจ้งให้ผู้ให้บริการทราบทุกครั้ง ก่อนการบันทึกการสนทนา
๕. การแจ้งปัญหา Gateway ไม่สามารถให้บริการได้หรือกรณีอื่นๆ	พัฒนาระบบส่ง Short Message เข้าโทรศัพท์มือถือของผู้บริหารหรือเจ้าหน้าที่ที่เกี่ยวข้อง
๖. สถานที่ให้บริการ	ผู้ให้บริการ Gateway เป็นผู้ดำเนินการและจัดหาสถานที่ให้บริการ พร้อมอุปกรณ์เครือข่ายที่เกี่ยวข้อง

## ส่วนวิจัยและพัฒนาเทคโนโลยีสารสนเทศ สำนักงานป้องกันและ ปราบปรามการฟอกเงิน

email : [cddgw@amlo.go.th](mailto:cddgw@amlo.go.th)

หมายเหตุ เพื่อความเข้าใจที่ตรงกันในการติดต่อประสานงาน จึงขอความร่วมมือให้ติดต่อผ่านทางอีเมลที่ระบุไว้  
ข้างต้นเท่านั้น

