



รายงานผลการรับฟังความคิดเห็นสาธารณะ
เรื่อง (ร่าง) มาตรฐานทางเทคนิคและ/หรือแนวปฏิบัติ
ด้านความมั่นคงปลอดภัยของโครงข่ายและระบบโทรคมนาคม

มีนาคม 2553

สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ

87 ถนนพหลโยธิน ซอย 8 (สายลม) แขวงสามเสนใน เขตพญาไท กรุงเทพมหานคร 10400

โทรศัพท์ 0 2271 0151-60 เว็บไซต์: www.ntc.or.th

สารบัญ

หน้า

ส่วนที่ 1	การจัดทำมาตรฐานทางเทคนิคและ/หรือแนวทางปฏิบัติด้านความมั่นคงปลอดภัยของโครงข่ายและระบบโทรคมนาคม (Network Security)	1
ส่วนที่ 2	สรุปความคิดเห็นจากรับฟังความเห็นสาธารณะเรื่อง (ร่าง) มาตรฐานทางเทคนิคและ/หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยของโครงข่ายและระบบโทรคมนาคมและข้อชี้แจงของคณะกรรมการฯ	3

ส่วนที่ 1

การจัดทำมาตรฐานทางเทคนิคและ/หรือแนวทางปฏิบัติ
ด้านความมั่นคงปลอดภัยของโครงข่าย
และระบบโทรคมนาคม (Network Security)

การจัดทำมาตรฐานทางเทคนิคและ/หรือแนวทางปฏิบัติด้านความมั่นคงปลอดภัย ของโครงข่ายและระบบโทรคมนาคม (Network Security)

1. ความเป็นมา

คณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กทช.) ได้แต่งตั้งคณะกรรมการมาตรฐาน กทช. เพื่อรับผิดชอบการศึกษา วิเคราะห์มาตรฐานทางด้านโทรคมนาคมและด้านอื่นที่เกี่ยวข้องใน ระดับสากล และเสนอแนะมาตรฐานที่เหมาะสมสำหรับประเทศไทย รวมทั้งการกำหนดมาตรฐานและ ลักษณะพึงประสงค์ทางด้านเทคนิคในกิจการโทรคมนาคมและกิจการวิทยุคมนาคม ซึ่งรวมถึงการ กำหนดมาตรฐานของระบบ โครงข่าย เครื่องโทรคมนาคมและอุปกรณ์ ตลอดจนถึงซอฟต์แวร์ โทรคมนาคมที่เกี่ยวข้อง จัดลำดับความสำคัญในการกำหนดมาตรฐานให้สอดคล้องและเหมาะสมกับ สภาพการณ์ โดยมีวาระในการปฏิบัติหน้าที่ 1 ปี ตามคำสั่งคณะกรรมการกิจการโทรคมนาคมแห่งชาติ ที่ 4/2552

คณะกรรมการมาตรฐาน กทช. ได้มีคำสั่งที่ 4/2552 ลงวันที่ 5 พฤศจิกายน 2552 เรื่อง แต่งตั้งคณะอนุกรรมการเฉพาะกิจจัดทำมาตรฐานทางเทคนิคด้านความมั่นคงปลอดภัยของโครงข่าย และระบบโทรคมนาคม (Network Security) โดยให้ดำเนินการยกร่างมาตรฐานทางเทคนิคและ/หรือ แนวทางปฏิบัติด้านความมั่นคงปลอดภัยของโครงข่ายและระบบโทรคมนาคม (Network Security) ให้ แล้วเสร็จภายใน 90 วัน หลังจากมีคำสั่งแต่งตั้งคณะอนุกรรมการฯ พร้อมทั้งจัดให้มีการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้มีส่วนเกี่ยวข้อง เกี่ยวกับร่างมาตรฐานทางเทคนิค และ/หรือ แนวทางปฏิบัติที่ได้จัดทำขึ้นและนำข้อคิดเห็น/ข้อเสนอแนะที่ได้รับไปพิจารณาปรับปรุงแก้ไขร่าง มาตรฐานทางเทคนิค และ/หรือ แนวทางปฏิบัติ ให้ครบถ้วนสมบูรณ์ ก่อนนำเสนอร่างที่ปรับปรุงแล้ว พร้อมรายงานสรุปผลการดำเนินงานต่อคณะกรรมการมาตรฐาน กทช. ภายใน 120 วันหลังจากมี คำสั่งแต่งตั้งคณะอนุกรรมการฯ

2. การดำเนินงาน

คณะอนุกรรมการเฉพาะกิจจัดทำมาตรฐานทางเทคนิคด้านความมั่นคงปลอดภัยของ โครงข่ายและระบบโทรคมนาคม (Network Security) ได้ประชุมรวมทั้งสิ้น 7 ครั้ง เพื่อพิจารณา หรือ ในประเด็นที่เกี่ยวข้องกับการจัดทำร่างมาตรฐานทางเทคนิค และ/หรือแนวทางปฏิบัติด้านความมั่นคง ปลอดภัยของโครงข่ายและระบบโทรคมนาคม รวมทั้งแนวทางการบังคับใช้และประเด็นกฎหมายที่ เกี่ยวข้อง โดยได้จัดทำร่างมาตรฐานทางเทคนิคและ/หรือแนวทางปฏิบัติที่สมควรใช้งานในประเทศไทย ซึ่งอ้างอิงเนื้อหาจากมาตรฐาน ITU-T Recommendation X.1051 (02/2008) Information technology – Security techniques – Information security management guidelines for telecommunications organization based on ISO/IEC 27002 ซึ่งประกอบด้วยแนวทางในการ ปฏิบัติตามและบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศสำหรับองค์กรที่ให้บริการ โทรคมนาคม และมาตรการในการรักษาความมั่นคงปลอดภัย รวมไปถึงแนวทางการบังคับใช้และ ประเด็นกฎหมายที่เกี่ยวข้องที่สมควรใช้งานในประเทศไทย เรียบร้อยตามกรอบระยะเวลาที่กำหนด

ในการประชุมคณะกรรมการมาตรฐาน กทช. ครั้งที่ 1/2553 เมื่อวันที่ 13 มกราคม 2553 ประธานอนุกรรมการฯ ได้นำเสนอร่างประกาศ ฯ ต่อคณะกรรมการมาตรฐาน กทช. เพื่อขอความเห็นชอบในการจัดรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียและผู้มีส่วนเกี่ยวข้อง

ต่อมาคณะอนุกรรมการฯ ในการประชุมครั้งที่ 2/2553 และครั้งที่ 3/2553 เมื่อวันที่ 18 และ 28 มกราคม 2553 ได้พิจารณาปรับปรุงร่างประกาศฯ และดำเนินการรวมร่างประกาศ ฯ 2 ฉบับเป็นฉบับเดียวกัน และมีมติให้จัดรับฟังความคิดเห็นฯ ในวันศุกร์ที่ 19 กุมภาพันธ์ 2553 เวลา 13.00 – 16.30 ณ.โรงแรมรามาร์คเดนิส กรุงเทพมหานคร ซึ่งมีผู้เข้าร่วมการจัดรับฟังความคิดเห็นที่มีการลงนามรับเอกสารรวมจำนวน 150 คน

3. ผลการจัดรับฟังความคิดเห็นสาธารณะ

การรับฟังความคิดเห็นสาธารณะ คณะอนุกรรมการฯ ได้นำเสนอประกาศซึ่งประกอบด้วยมาตรฐานทางเทคนิคในการรักษาความมั่นคงปลอดภัยของโครงข่ายฯ และมาตรการขั้นต่ำที่จะบังคับใช้กับผู้ประกอบกิจการโทรคมนาคมแต่ละกลุ่ม

จากการพิจารณาความเห็นและข้อเสนอทั้งหมดที่ได้รับจากการจัดรับฟังความคิดเห็นสาธารณะ คณะอนุกรรมการฯ เห็นควรปรับปรุงมาตรฐานที่ยกสร้างขึ้นให้เป็นร่างแนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยทางสารสนเทศสำหรับองค์กรด้านโทรคมนาคม และชะลอการบังคับใช้มาตรการขั้นต่ำไว้ก่อน อนึ่งคณะอนุกรรมการฯ ได้แก้ไขเนื้อหาแนวปฏิบัติฯ ในส่วนคำนิยามและที่เกี่ยวข้องให้ชัดเจนยิ่งขึ้น และจัดส่งร่างฉบับสมบูรณ์ให้สำนักงานฯ ต่อไป ในส่วนประเด็นข้อคิดเห็นฯ คณะอนุกรรมการฯ ได้จัดทำข้อชี้แจงในรายละเอียดปรากฏในส่วนที่ 2 ของรายงานฉบับนี้

4. สรุป

คณะอนุกรรมการฯ ได้จัดทำมาตรฐานและมาตรการขั้นต่ำที่จะบังคับใช้ตามขั้นต่ำในลักษณะที่เป็น CMMI (Capability Maturity Model Integration) อย่างไรก็ดีตามเมื่อประมวลผลจากข้อคิดเห็นทั้งหมดที่ได้รับจากการรับฟังความคิดเห็นสาธารณะ คณะอนุกรรมการฯ เห็นว่าในระยะเริ่มแรกควรใช้เอกสารเป็นแนวปฏิบัติไปก่อนเพื่อให้อ้างอิงในการปฏิบัติ ส่วนการบังคับใช้มาตรการขั้นต่ำ จะชะลอไว้ก่อนและนำกลับไปศึกษาเพิ่มเติม หากจะมีการนำมาบังคับใช้

ส่วนที่ 2

สรุปความคิดเห็นจากรับฟังความเห็นสาธารณะเรื่อง (ร่าง) มาตรฐานทาง
เทคนิคและ/หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยของโครงข่ายและระบบ
โทรคมนาคมและข้อชี้แจงของคณะอนุกรรมการฯ

สรุปความคิดเห็นจากรับฟังความเห็นสาธารณะ
เรื่อง (ร่าง) มาตรฐานทางเทคนิคและหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยของ
โครงข่ายและระบบโทรคมนาคมเมื่อวันที่ 19 กุมภาพันธ์ 2553
และข้อชี้แจงของคณะกรรมการ

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
1.	ผู้เข้าร่วม สัมมนา (ไม่ได้ แจ้งชื่อ)	ITU-T X.1051 ซึ่งชื่อภาษาอังกฤษเป็น Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 ทำไมชื่อภาษาไทยจึงแปลเป็นความมั่นคง ปลอดภัยของโครงข่ายและระบบ โทรคมนาคม โดยไม่มีคำว่า “สารสนเทศ” แต่เพิ่มคำว่า “โครงข่าย”เข้ามา กรุณา อธิบายที่มาและเหตุผล	จะแก้ไขให้สอดคล้องกับชื่อภาษาอังกฤษ ITU-X.1051 เป็น “แนวปฏิบัติในการ บริหารจัดการความมั่นคงปลอดภัยทาง สารสนเทศสำหรับองค์กรด้าน โทรคมนาคม ”
2	ผู้แทน บมจ. โท เท็ล แอ็คเซ็ส คอมมูนิเคชั่น (ดีแทค)	2.1 ขอให้มีการนำสรุปความคิดเห็นที่ได้รับ ในวันนี้และคำชี้แจงของคณะกรรมการ มาเผยแพร่ในเว็บไซต์ ของ กทช. ตาม ระเบียบของสำนักงาน กทช. 2.2 โดยเนื้อหาและขอบเขตเกี่ยวกับ มาตรฐานทางเทคนิคความมั่นคงฯนี้ ครอบคลุมเนื้อหาหลายส่วนซึ่งไม่ใช่เนื้อหา ด้านเทคนิค เช่น การสรรหาบุคคลเข้า ทำงาน 2.3 กฎเกณฑ์นี้ยังไม่ชัดเจน น่าจะใช้ ระยะเวลา 1 ปี ที่กำหนดให้มีผลบังคับใช้ ไปในการเตรียมพร้อมและพิจารณา ปรับปรุงกฎเกณฑ์ให้ชัดเจน ไม่ควรเร่งรีบ ออกประกาศ 2.4 ตามที่อนุกรรมการฯ กล่าวว่า ปัจจุบัน มีผู้ประกอบการบางรายได้ดำเนินการตาม	2.1 สำนักงานฯ จะได้สรุปความเห็น และ คำชี้แจงทั้งหมด และดำเนินการตาม ระเบียบ กทช. ที่เกี่ยวข้องต่อไป 2.2 ได้แก้ไขให้เอกสารมีสถานะเป็นแนว ปฏิบัติ (guideline) แล้ว 2.3 ได้แก้ไขให้เอกสารมีสถานะเป็นแนว ปฏิบัติ (guideline) แล้ว และจะได้ปรับปรุงเนื้อหาให้ชัดเจนยิ่งขึ้น 2.4 สามารถตรวจสอบรายชื่อหน่วยงาน ที่ได้นำระบบ ISO 27001 ไปปฏิบัติและ

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>มาตรฐานด้านความมั่นคงปลอดภัยของ โครงข่ายฯ แล้ว อยากให้ระบุว่า ผู้ประกอบการรายไหนทำ แล้วหรือยังไม่ ทำ การที่ให้ทุกรายทำเหมือนกันหมดนั้น อาจจะมีปัญหา เพราะ ในส่วนที่ 2 มาตรการขั้นต่ำฯ ในข้อ 6 กำหนดว่า “ ผู้ ประกอบกิจการที่ใช้โครงข่ายและระบบ โทรคมนาคมของผู้ให้บริการ ให้บริการ มี หน้าที่ต้องกำหนดให้ผู้ประกอบการที่ตน ใช้โครงข่ายและระบบโทรคมนาคมอยู่ ดำเนินการให้เป็นไปตามมาตรการฯ ฉบับ นี้ด้วย” นั้น เหมือนเป็นการบังคับใช้กับทุก ราย ผู้ประกอบการจะใช้อำนาจอะไรในการ บังคับกับบุคคลที่สาม ซึ่งผู้ประกอบการไม่ สามารถทำได้</p> <p>2.5 ในส่วนที่ 2 มาตรการขั้นต่ำฯ นิยาม เกณฑ์ของบริการด้านโทรคมนาคมที่สำคัญ มาก/บริการด้านโทรคมนาคมที่เป็นจุด วิกฤต (Critical Service) ข้อ 2 ที่กำหนด ว่า “1. บริการด้านการสื่อสารที่มีโครงสร้าง พื้นฐานเป็นของตนเอง หรือใช้พื้นฐานของ ผู้ให้บริการรายอื่น โดยที่โครงสร้างนี้ทำ หน้าที่เป็น Backbone ของประเทศตามที่ กทช. ได้กำหนดไว้” ไม่มีความชัดเจน เนื่องจากปัจจุบันทาง กทช. ยังไม่มีการ กำหนดโครงสร้างที่ทำหน้าที่เป็น Backbone ของประเทศ</p> <p>2.6 ในส่วนที่ 2 มาตรการขั้นต่ำฯ ในข้อ 10 “การประกอบกิจการโทรคมนาคมและ ให้บริการอินเทอร์เน็ตของผู้ที่ได้รับอนุญาต สัมปทาน หรือสัญญาตามมาตรา 80 แห่ง</p>	<p>ได้รับการรับรองแล้ว ได้จากเว็บไซต์ www.iso27001certificates.com โดย เลือกเมนู Certificate Register สำหรับเนื้อหาส่วนที่ 2 มาตรการขั้นต่ำฯ นั้นจะ ชะลอไว้ก่อนและนำกลับไปศึกษา เพิ่มเติม</p> <p>2.5 เป็นการแก้คำผิด เป็น Backbone ที่ กทช. กำหนด สำหรับเนื้อหาส่วนที่ 2 มาตรการขั้นต่ำฯ นั้นจะ ชะลอไว้ก่อนและ นำกลับไปศึกษาเพิ่มเติม</p> <p>2.6 จะแก้ไขให้สอดคล้องกับ มาตรา 80 แห่งพระราชบัญญัติการประกอบกิจการ โทรคมนาคม พ.ศ. 2544 สำหรับเนื้อหา ส่วนที่ 2 มาตรการขั้นต่ำฯ นั้นจะชะลอไว้</p>

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 ต้องอยู่ภายใต้หลักเกณฑ์และเงื่อนไขตามประกาศนี้ ในกรณีนี้ ให้ถือว่าผู้ที่ได้รับอนุญาตสัมปทาน หรือสัญญาอันมีหน้าที่ต้องดำเนินการให้เป็นไปตามประกาศนี้ด้วย”</p> <p>ข้อมูลอาจไม่ตรงกับข้อเท็จจริง ผู้ที่ได้รับสัมปทานอินเทอร์เน็ตนั้นไม่มีในปัจจุบัน ซึ่ง กทช ออกกฎเกณฑ์ มาเพื่อบังคับใช้กับผู้รับใบอนุญาตเท่านั้น</p>	ก่อนและนำกลับไปศึกษาเพิ่มเติม
3.	ผู้แทน บมจ.กสท. โทรคมนาคม	<p>3.1 แนวคิดในการจัดการระบบโทรคมนาคม เราจะให้ระบบมีความมั่นคงปลอดภัย โดยมาตรฐาน นี้ไม่ได้ระบุ หัวใจสำคัญของมาตรฐาน 27001 Information security management system- Requirements นั้นคือ การประเมิน ความเสี่ยง (Risk assessment) โดยเลือกมาตรการ (control) มาใช้ อนุกรรมการใช้หลักการอะไรในการ เลือกมาตรการ (control) เพราะผู้ใช้มาตรฐาน 27001 นั้นใช้การจัดการความเสี่ยงเป็นหัวใจสำคัญ โดยที่มาตรการ(control) เหล่านี้ เป็นแค่ guideline ไม่ได้เป็นข้อบังคับ อย่างไรก็ตาม มาตรฐานฉบับนี้เป็นการใช้ที่ไม่ได้นำหัวใจสำคัญในหลายประเด็น โดยเฉพาะการประเมินความเสี่ยงมาด้วย และไม่ได้อ้างอิงมาตรฐาน ISO 27001 ซึ่งได้รับการยอมรับในระดับสากล</p>	3.1 รับทราบความเห็น

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>3.2 การที่จะให้ผู้ประกอบการกลุ่ม ก ทำ ทุก 143 มาตรการ นั้น ไม่เห็นด้วย เนื่องจากอนุกรรมการกล่าวว่ มาตรฐาน ฉบับนี้เน้น Availability หากเป็นเช่นนั้น ควรจะให้มีความสำคัญ กับมาตรการด้าน Business continuity</p> <p>3.3 ระยะเวลา 12 เดือน ในการปรับตัว นั้นน้อยเกินไป เพราะปกติ บริษัท จะใช้ เวลา 2-3 ปี ในการวางแผนงาน แล้วมา วิเคราะห์ความเสี่ยงในแต่ละปี</p> <p>3.4 น่าจะศึกษาว่า แต่ละ operator มีความ เข้าใจต่อแก้ไขในมาตรฐานที่จะนำมาบังคับ ใช้แล้วรียัง ควรศึกษาผลกระทบที่เกิดขึ้น ในประเทศอื่น ๆ ที่มีการนำมาตรฐาน เช่นเดียวกันนี้ไปใช้ และควรจะต้องศึกษาผลกระทบกับ operator ทุกรายที่โดนบังคับใช้ เพื่อให้มี ความชัดเจน เพราะมาตรการที่เกิดขึ้นนั้น จะเป็นค่าใช้จ่ายในการลงทุนที่มีมูลค่าสูง ซึ่ง operator อาจจะผลกระทบไปให้ ผู้บริโภค</p> <p>3.5 ควรมีการกำหนด ความถี่ในการสุ่ม ตรวจ รวมทั้งกำหนดแผนและวิธีการตรวจ อย่างชัดเจนอ้างอิงตามหลัก มาตรฐานสากล และรวมถึงควรมีการ แต่งตั้งคณะกรรมการตรวจสอบกลางอิสระ ซึ่งประกอบด้วยผู้ที่มีคุณวุฒิและได้รับ ประกาศนียบัตรมาตรฐานสากลจาก หน่วยงานกลาง รวมถึงไม่เป็นผู้ที่มีส่วนได้ ส่วนเสียหรือมีผลประโยชน์ในทางธุรกิจกับ ผู้ประกอบการโทรคมนาคม</p>	<p>3.2 สำหรับเนื้อหาส่วนที่ 2 มาตรการชั้น ต่ำนั้นจะชะลอไว้ก่อนและนำกลับไป ศึกษาเพิ่มเติม</p> <p>3.3 เนื่องจากได้แก้ไขเป็นแนวทางปฏิบัติ และเนื้อหาส่วนที่ 2 มาตรการชั้นต่ำนั้น จะ ชะลอไว้ก่อนและนำกลับไปศึกษา เพิ่มเติม</p> <p>3.4 รับทราบความเห็นและอาจจะมีการ จัด workshop เพื่อสร้างความเข้าใจ ให้กับ operator ต่อไป</p> <p>3.5 ได้ทำเป็นแนวปฏิบัติแล้วซึ่งจะยังไม่ มีการสุ่มตรวจ</p>

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>3.6 อนุกรรมการมีหลักเกณฑ์อย่างไรในการเลือกมาตรการต่างๆว่าทำ 99 ข้อ 41 ข้อ ออกมาบังคับที่จำแนกตามใบอนุญาต เป็น กลุ่ม ก ข ค โดย มาตรการข้อที่ไม่ได้ประกาศบังคับไว้ อาจจะเป็น มาตรการที่จำเป็นสำหรับผู้ประกอบการ บางรายที่มีความเสี่ยงในด้านนั้น</p> <p>3.7 การรับรองตนเองนั้นไม่สามารถยืนยันได้อย่างแท้จริงตามที่ได้รายงานไว้</p>	<p>3.6 ได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว สำหรับเนื้อหา ส่วนที่ 2 มาตรการขั้นตํานั้นจะชะลอและ นำกลับไปศึกษาเพิ่มเติม</p> <p>3.7 กำหนดเป็นการรับรองตนเองนั้น เป็นแนวทางเดียวกับประกาศ กทช. ใน เรื่อง หลักเกณฑ์และมาตรการกำกับดูแล ความปลอดภัยต่อสุขภาพของมนุษย์จากการใช้เครื่องวิทยุคมนาคม อย่างไรก็ตาม เนื่องจากเป็นแนวปฏิบัติ จึงยังไม่มี การบังคับให้มีการรับรองตนเอง</p>
4.	ผู้แทน บริษัท ทรู	<p>4.1 มาตรฐานฉบับนี้คณะอนุกรรมการฯ มีความตั้งใจจะเป็น guideline หรือ เป็น มาตรฐานที่บังคับใช้</p> <p>ในการนำเสนอของอนุกรรมการฯ ได้มีข้อมูล แสดงว่า ในต่างประเทศ อาทิ สวิสเซอร์แลนด์และญี่ปุ่นใช้มาตรฐาน ITU-X.1051 เป็นแนวทางปฏิบัติ(ไม่ใช่กฎที่ บังคับใช้) ดังนั้นจึงอยากให้พิจารณาว่าใน ต่างประเทศนั้น มีการบังคับใช้ที่ประเทศ ไตบ้าง</p> <p>4.2 เห็นด้วย ที่อนุกรรมการเห็นว่า Availability เป็นเรื่องที่สำคัญกับผู้บริโภค โดยที่ผู้ให้บริการให้ความสำคัญอยู่แล้ว อยากให้พิจารณา ว่าการแข่งขันในการให้ คุณภาพบริการ จะช่วยในเรื่อง Availability ดังนั้น อยากให้พิจารณาว่ากฎเกณฑ์เรื่อง การแข่งขันต่างๆ ของ กทช. ปัจจุบัน เพียงพอหรือยัง ก่อนที่จะนำเรื่อง</p>	<p>4.1 ได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว</p> <p>4.2 รับทราบความเห็น</p>

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>มาตรฐานด้านความมั่นคงปลอดภัยของ โครงข่ายมาบังคับใช้</p> <p>4.3 คิดว่ามาตรฐานนี้เป็นสิ่งที่ดีใน ระยะแรก อาจจะมีการจัด workshop สร้างความรู้ ความเข้าใจ หรือรณรงค์ให้ ผู้ประกอบการเห็นความสำคัญ เพื่อที่ ผู้ประกอบการสามารถนำมาใช้เป็น reference ได้</p>	<p>4.3 รับทราบและจะนำเสนอ คณะกรรมการมาตรฐาน กทช ต่อไป</p>
5	ผู้แทนบริษัท เบญจจินดาฯ	<p>5.1 อยากทราบว่า กทช จะอาศัยฐาน อำนาจข้อไหนในการนำมาตรฐานฉบับนี้มา บังคับใช้</p> <p>5.2 มาตรฐานฉบับนี้จะนำมาบังคับใช้ หรือ เป็นแนวทางปฏิบัติ</p> <p>5.3 หากบังคับใช้ แล้วจะซ้ำซ้อนกับทาง กระทรวงเทคโนโลยีสารสนเทศ ฯ หรือ เปล่า เช่น หาก ทำผิดประกาศของ กทช แล้วจะทำผิดประกาศของ กระทรวง เทคโนโลยีสารสนเทศ ฯ ด้วยหรือไม่</p> <p>5.4 จำนวนมาตรการที่บังคับใช้มีเป็น จำนวนมาก จะสร้างภาระและต้นทุนต่อ องค์กรเป็นอย่างมาก</p> <p>5.5 ในส่วนที่ 2 มาตรการขั้นต่ำๆ ข้อ 8 “ ในกรณีที่ผู้ประกอบการไม่ปฏิบัติตาม ข้อกำหนดในประกาศนี้ เลขานุการอาจมี คำสั่งให้ผู้ประกอบการดังกล่าว ดำเนินการให้เป็นไปตามประกาศนี้ภายใน</p>	<p>5.1 ถ้าหากจะมีการบังคับใช้ในอนาคต กทช จะมีอำนาจออกประกาศฉบับนี้ ขึ้นอยู่กับว่า เนื้อหาเป็นมาตรฐานทาง เทคนิคทางโครงข่ายโทรคมนาคม ตาม มาตรา 32 และมาตรา 33 หรือไม่</p> <p>5.2 ได้แก้ไขให้เอกสารมีสถานะเป็นแนว ปฏิบัติ (guideline) แล้ว</p> <p>5.3 หากจะบังคับใช้ ขึ้นอยู่กับข้อเท็จจริง ว่าผิดกฎหมายฉบับใด</p> <p>5.4 รับทราบความเห็น</p> <p>5.5 เนื้อหาส่วนที่ 2 มาตรการขั้นต่ำนั้น จะ ชะลอไว้ก่อนและนำกลับไปศึกษา เพิ่มเติม</p>

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>ระยะเวลาที่กำหนดก็ได้” หากผู้ประกอบการเห็นว่า กทช ไม่มีอำนาจในการบังคับใช้ประกาศนี้และไม่ปฏิบัติตามใครจะเป็นผู้รับผิดชอบ ในเรื่องการฟ้องร้องที่อาจเกิดขึ้นต่อไป ดังนั้นจึงอยากให้พิจารณาฐานอำนาจให้รอบคอบ</p> <p>5.6 พรบ. การประกอบกิจการ พ.ศ. 2544 มาตรา32และ33 เป็นการกำหนดมาตรฐานทางเทคนิคของประเภทของโครงข่ายโทรคมนาคม เครื่องโทรคมนาคมและอุปกรณ์ที่ใช้ในกิจการโทรคมนาคม ไม่ใช่เรื่องที่เกี่ยวข้องกับการบริหารงานในภายในองค์กร หรือภายในสำนักงาน ดังนั้นจึงอยากขอให้พิจารณาความหมายให้ชัดเจน</p>	<p>5.6 รับทราบความเห็นและได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว</p>
6.	ผู้แทนบริษัท ทรูๆ	<p>6.1 ตามที่อนุกรรมการได้นำเสนอมาตรฐานฉบับนี้ที่ อ้างอิงจาก ITU-T X.1051 นั้น ถ้าความเข้าใจของผู้ประกอบการ หรือความเข้าใจของ กทช ต่อ ITU-T x1051 ไม่ตรงกัน จะให้ยึดมาตรฐานไหนเป็นหลัก แล้วจะยึด ฉบับภาษาไทยของ กทช หรือ ฉบับของ ITU-T เป็นหลัก</p> <p>6.2 เนื้อหามาตรการบางข้อ ขัดแย้งกัน เช่น ส่วนที่ 1 ข้อ 4.2.4.3 กำหนดให้ทำการประเมินความเสี่ยง แล้วเลือกมาตรการที่เหมาะสมมาปฏิบัติสำหรับองค์กร แต่ในส่วนที่ 2 มาตรการขั้นต่ำให้บังคับปฏิบัติตามมาตรการที่กำหนด</p> <p>6.3 มาตรการแต่ละข้อ ปฏิบัติอย่างไรจึงจะเรียกว่าปฏิบัติแล้ว แล้วปฏิบัติแค่ไหนจึงจะ</p>	<p>6.1 หากบังคับใช้ ต้องยึดฉบับภาษาไทยตามร่างประกาศของ กทช. ทั้งนี้หากคิดว่า การแปลคำใดไม่ตรง ก็สามารถแสดงความคิดเห็นมาได้</p> <p>6.2 ได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว สำหรับเนื้อหาส่วนที่ 2 มาตรการขั้นต่ำนั้นจะชะลอไว้ก่อนและนำกลับไปศึกษาเพิ่มเติม</p> <p>6.3 ปฏิบัติตามระดับความเสี่ยงของผู้ประกอบการเอง</p>

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>ถือว่าเป็นระดับที่พอเพียง</p> <p>6.4 ควรมีความชัดเจนว่าจะให้ปฏิบัติอะไร หรือว่าไม่ปฏิบัติอะไร เพราะในเนื้อหาส่วนใหญ่เป็น “ควร” ซึ่งต้องใช้ดุลยพินิจ</p> <p>6.5 เรื่องวัตถุประสงค์ในการปฏิบัติตามมาตรฐานนั้นเห็นด้วยว่าเป็นผลดี การนำมาตรฐานมาใช้ควรจะสอดคล้องสภาพความเป็นจริงและ ต้องเข้าใจถ่องแท้ว่าจริงๆแล้วปฏิบัติอย่างไร มีการวัดผลอย่างไร</p>	<p>6.4 ได้แก้ไขให้มีความชัดเจนมากขึ้น โดยแนวปฏิบัติทั้งหมดใช้คำว่า “ควร”</p> <p>6.5 รับทราบความเห็นและจะหาแนวทางส่งเสริมและพัฒนาอุตสาหกรรมต่อไป</p>
7.	ผู้แทนบริษัท ทรูๆ	<p>7.1 มาตรการที่ออกมาจะมีผลบังคับใช้ย้อนหลังหรือเปล่า</p> <p>เช่น ข้อ 9.1.9 “การสร้างความมั่นคงปลอดภัยสำหรับพื้นที่ปฏิบัติการด้านโทรคมนาคม” นั้นอาจจะไม่เหมาะสม เพราะยากที่จะทำได้</p> <p>ส่วนข้อ 9.1.8 ในเรื่องของการปลอดภัยของห้องอุปกรณ์โทรคมนาคม บางที่อุปกรณ์ไม่ได้อยู่ในห้องแล้ว อยู่ข้างถนนก็มี ดังนั้นก็ยากที่จะทำได้</p>	<p>7.1 หากมีการบังคับใช้ จะขึ้นอยู่กับข้อเท็จจริง ตามหลักกฎหมาย หากผลที่เกิดขึ้น สร้างความเสียหายอันมีอาจหลีกเลี่ยงได้ ก็อาจจะไม่ย้อนหลัง เช่น อาคารเก่าแล้วไม่มีแผนงานที่จะสร้างอาคารใหม่ แต่ทั้งนี้ต้องมีมาตรการรักษาความมั่นคงปลอดภัยอื่นที่เพียงพอ</p>
8.	ผู้แทนสมาคม ความมั่นคง ปลอดภัยระบบ สารสนเทศ (TISA)	<p>8.1 เนื้อหา ของคำแปลคำเดียวกันมีคำแปลที่ไม่สอดคล้องกันอยู่หลายแห่ง เช่น Asset บางหัวข้อแปลเป็นทรัพย์สิน บางหัวข้อ แปลเป็น ทรัพย์สินสารสนเทศ นั้นดูไม่สอดคล้องกัน</p> <p>8.2 ในเนื้อหานั้น ควรจะ ให้ความสำคัญไปที่ความเสี่ยง ของแต่ละผู้ประกอบการ ไม่ควรให้ความสำคัญเฉพาะเรื่อง มาตรการ ที่ต้องปฏิบัติเท่านั้น</p>	<p>8.1 จะได้ปรับปรุงให้เหมาะสมต่อไป</p> <p>8.2 รับทราบความเห็น</p>

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		8.3 มาตรฐานฉบับนี้ จะใช้คำว่าอะไร ระหว่างควรทำ หรือว่าต้องทำ โดย should แปลว่า ควร shall แปลว่า ต้อง ดังนั้น น่าจะมีการทำความเข้าใจให้ตรงกันก่อนที่จะนำมาใช้ประกาศ	8.3 รับทราบความเห็น
9.	ผู้แทน บมจ. แอดวานซ์อินโฟร์เซอร์วิส (AIS)	<p>9.1 น่าจะต้องมีระดับความเข้มข้นและการกำหนดว่าจะต้องทำอะไรบ้างให้ชัดเจน เพราะการลงทุนด้านความมั่นคงปลอดภัยนั้นมีค่าใช้จ่ายสูงมาก หากไม่มีมาตรฐานที่เท่าเทียมกัน ไม่สามารถต่างคนต่างตีความได้</p> <p>9.2 น่าจะมีมาตรการที่จะต้องชัดเจน รายจ่ายที่ลงทุนไป เช่น ชดเชย ค่า license หรือไม่ ก็มาตรการทางภาษีที่สนับสนุนผู้ประกอบการ</p> <p>9.3 เรื่องชื่อของมาตรฐาน นั้นอาจจะไม่ครอบคลุม เพราะ ในเนื้อหาไม่ได้มีเฉพาะโครงข่ายโทรคมนาคม อาจจะรวมถึงระบบไอทีในองค์กร และอุปกรณ์ทางคอมพิวเตอร์อื่นๆด้วย</p>	<p>9.1 ได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว สำหรับเนื้อหาส่วนที่ 2 มาตรการขั้นตานั้นจะชะลอไว้ก่อนและนำกลับไปศึกษาเพิ่มเติม</p> <p>9.2 รับทราบความเห็น</p> <p>9.3 ได้แก้ไขชื่อให้สอดคล้องกับชื่อมาตรฐาน ITU X.1051 Information security management guidelines</p>
10.	ผู้แทน บมจ.กสท. โทรคมนาคม	10.1 ในเรื่องของการประเมินความเสี่ยง มีมาตรการ หรือขั้นตอนอย่างไร ในการบอกว่า วิกฤตหรือไม่วิกฤต แนวทางการตรวจสอบ ระดับความเข้มข้น แต่ไหนถึงจะเข้าสู่เกณฑ์มาตรฐานที่วางไว้	10.1 รับทราบความเห็น
11.	ผู้แทนบริษัท เบญจจินดาฯ	11.1 หากคณะอนุกรรมการเห็นว่าจะต้องบังคับใช้ เห็นว่ามีเรื่องเดียวคือเรื่องการบริหารจัดการความต่อเนื่องทางธุรกิจที่ น่าจะบังคับใช้เพียงอย่างเดียวเท่านั้น ส่วนเรื่องอื่นๆนั้น กระทรวงเทคโนโลยีสารสนเทศ หรือ หน่วยงานอื่นจะเป็นผู้ดูแลอยู่แล้ว ไม่ควรมากำกับดูแลซ้ำซ้อน	11.1 ได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว สำหรับเนื้อหาส่วนที่ 2 มาตรการขั้นตานั้นจะชะลอไว้ก่อนและนำกลับไปศึกษาเพิ่มเติม

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
12.	ผู้แทนบริษัท ทฤษฎ	12.1 เรื่องการบังคับใช้นั้น ถ้าเกิดมีการประกาศลงราชกิจจานุเบกษา แล้วจะแก้ไขได้ยากมาก ดังนั้นจึงขอให้พิจารณาให้รอบคอบ	12.1 จะยังไม่มี การบังคับใช้
13.	ผู้แทนสมาคม ความมั่นคง ปลอดภัยระบบ สารสนเทศ (TISA)	13.1 เรื่องประเด็นรูปแบบ ของเอกสาร นั้น อาจจะ ไม่พร้อมใช้งาน ทั้งการแปล เรื่องการใช้ชื่อภาษาไทยและภาษาอังกฤษ มีความคลาดเคลื่อน เนื้อหาไม่ชัดเจน 13.2 เห็นว่าเรื่องความมั่นคงปลอดภัยนั้น เกี่ยวข้องบุคคล อาจจะมีข้อกำหนดให้ ผู้ประกอบการพัฒนาบุคลากรให้ความเชี่ยวชาญทางด้านความมั่นคงปลอดภัย ในระดับที่สากลยอมรับ เพราะประเทศไทย มีผู้เชี่ยวชาญด้านนี้ น้อยมาก	13.1 จะปรับปรุงให้เหมาะสมยิ่งขึ้นต่อไป 13.2 รับทราบและจะเสนอ ให้มีการพัฒนาบุคลากรในด้านนี้ต่อไป
14.	ผู้เข้าร่วม สัมมนา (ไม่ได้ แจ้งชื่อ)	14.1 การบังคับใช้ นั้น เป็นประเด็นโต้แย้งที่สำคัญโดยสภาพของมาตรฐานนั้นเป็น การบริหารจัดการ ซึ่งไม่สามารถใช้บังคับได้ เพราะไม่สามารถชี้ชัดได้ว่าองค์กรใดควรปฏิบัติอย่างไร การบริหารจัดการนั้น ต้องใช้ดุลยพินิจและปัจจัยอื่นๆที่เกี่ยวข้อง และการมีการจัดการบริหารที่ดีนั้นไม่ได้ชี้ชัดว่าใครจะมีความมั่นคงปลอดภัย ถ้ามีหลักเกณฑ์ใดที่สามารถวัดผลได้ว่า ความปลอดภัยของโครงข่ายโทรคมนาคม เป็นอย่างไร	14.1 ได้แก้ไขให้เอกสารมีสถานะเป็นแนวปฏิบัติ (guideline) แล้ว สำหรับเนื้อหาส่วนที่ 2 มาตรการขั้นต่ำนั้นจะชะลอไว้ก่อนและนำกลับไปศึกษาเพิ่มเติม
15.	ผู้แทนบริษัท เบญจจินดา ฯ	15.1 มาตรฐาน ITU นั้น ไม่ได้เป็นมาตรฐานที่ให้ประเทศสมาชิกนั้นต้องปฏิบัติตาม เป็นแค่ สิ่งที่แสดงให้เห็นว่าการบริหารจัดการด้านโทรคมนาคมที่ดี เป็นอย่างไร ซึ่ง ผู้ประกอบการสามารถเลือกนำมาใช้ได้	15.1 รับทราบ

ลำดับ	ผู้แสดง ความเห็น	ความคิดเห็น/เหตุผล	ข้อชี้แจง/แนวทางดำเนินการ
		<p>15.2 การแยกระหว่างการกำกับดูแลโครงข่ายและข้อมูล(Information) นั้นสามารถแยกออกได้ เช่น หน้าทีของ กทช นั้น เป็นเรื่องของโครงข่ายที่สามารถให้บริการได้อย่างต่อเนื่อง หากเกิดภัยพิบัติ เช่น สายขาด ไฟไหม้ น้ำท่วม ทางผู้ประกอบการจะต้องทำอะไรเพื่อให้มีการสื่อสารโทรคมนาคมได้อย่างต่อเนื่อง อย่างเช่น ต้องมีรถสื่อสารดาวเทียม หรือ ต้องรีบ แก้ไข โดยเร็ว</p> <p>ส่วนเรื่องข้อมูล (Information) นั้น ควรจะต้องเป็นเรื่องของกระทรวงเทคโนโลยีสารสนเทศ จึง อยากให้แยกหน้าที่ชัดเจน เพราะหน้าที่อาจจะซ้ำซ้อน กันได้ ระหว่าง กทช กับ กระทรวงเทคโนโลยีสารสนเทศ ได้</p>	<p>15.2 หากร่างประกาศจะบังคับใช้ จะปรับปรุงร่างให้อยู่ให้ขอบอำนาจของ กทช.</p>
16.	ผู้แทน บมจ. แอดวานซ์อินโฟร์เซอร์วิส (AIS)	<p>16.1 การนิยาม asset นั้น น่าจะมีการระบุขอบเขตให้ชัดเจน เพราะว่า asset บางอย่าง มีความหมายกว้าง เช่น router จะรวมไปถึง layer2 ด้วยหรือเปล่า transmission จริงๆ ต้องอยู่ในนั้นหรือเปล่านั้น ตัวคอมพิวเตอร์จะเฉพาะแค่ CPU หรืออุปกรณ์ต่อพ่วงทั้งหมดหรือเปล่า</p>	<p>16.1 จะปรับปรุงให้เหมาะสมยิ่งขึ้นต่อไป</p>

หมายเหตุ : ภายหลังจากวันที่ 19 กุมภาพันธ์ 2553 สำนักงาน กทช. ได้รับหนังสือแสดงความคิดเห็นอย่างเป็นทางการเพิ่มเติม ซึ่งสาระสำคัญของหนังสือนั้นเป็นประเด็นที่ผู้แสดงความคิดเห็นด้วยวาจาในที่ประชุมแล้ว