GUIDELINE TO THE MINISTRIES, CENTRAL AGENCIES AND REGULATORY BODIES TO PROVIDE COMPLIANCE INSTRUCTIONS FOR THE MS ISO/IEC 27001:2007 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) IMPLEMENTATION

DRAFT

MS ISO/IEC 27001:2007 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) IMPLEMENTATION

Background

1. The *Jemaah Menteri* has decided on 24 February 2010, through their Memorandum, that the Critical National Information Infrastructure (**CNII**) entities of Malaysia to be MS ISO/IEC 27001:2007 Information Security Management System (**ISMS**) certified within 3 years from this date.

Next Steps

2. All Ministries, Central Agencies and Regulatory Bodies (hereby referred to as Governing Agencies) that have jurisdiction over, or are responsible to provide guidance and instructions to the CNII entities, are to notify the CNII entities under their purview/coverage pertaining to the *Jemaah Menteri's* decision.

3. All Governing Agencies are to identify the entities in their respective sectors to be notified. The National Cyber Security Policy (**NCSP**) identified the CNII entities as those whose services or products have critical impact to the nation, the public and the economy, if such services or product are disrupted.

4. In monitoring the progress of the implementation, Governing Agencies are to request and assemble information on compliance from the CNII entities from time to time to be reported to the National Cyber Security Coordination Committee (**NC3**) and the National Cyber Security Advisory Committee (**NaCSAC**). This also includes reporting any issues or problems faced in complying with the decision of the *Jemaah Menteri*.

5. As an initial step, the Governing Agencies are to instruct the respective CNII entities to provide the scope of the ISMS certification within two months from the notification. This information will be reported in the NC3 meeting in the second quarter of 2010.

List of Documents

6. Please find attached the relevant documents for the discussions:
   a) **ATTACHMENT 1: DRAFT OF THE LETTER TO THE GOVERNING AGENCIES ON THE ISMS CERTIFICATION**

Status of This Document

7. This document has not been discussed and endorsed to be sent out. It is meant to be the basis for discussion and consensus on the approach and details to communicate to the Governing Agencies.

ATTACHMENT 1

DRAFT OF THE LETTER TO THE GOVERNING AGENCIES ON THE ISMS CERTIFICATION

Rujukan Kami:

Tarikh:

SEPERTI SENARAI EDARAN

Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan,

PELAKSANAAN MS ISO/IEC 27001:2007 PENGURUSAN SISTEM KESELAMATAN MAKLUMAT (*INFORMATION SECURITY MANAGEMENT SYSTEM* - ISMS) UNTUK SEKTOR-SEKTOR PRASARANA MAKLUMAT KRITIKAL NEGARA (*CRITICAL NATIONAL INFORMATION INFRASTRUCTURE* - CNII)

Dengan hormatnya saya merujuk kepada perkara di atas dan Mesyuarat Jawatankuasa Penyelaras Keselamatan Siber Nasional (*National Cyber Security Coordination Committee* - NC3) Bil. 1/2010 pada 24 Mac 2010.

2. Dimaklumkan bahawa satu Bengkel membincangkan Pelaksanaan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (Information Security Management System - ISMS) untuk sektor-sektor Prasarana Maklumat Kritikal Negara (Critical National Information Infrastructure - CNII) akan diadakan seperti berikut :

Tarikh	**:**	**26 April 2010**
Masa	**:**	**9.00 am – 5.00 pm**
Tempat	**:**	**BILIK LATIHAN AKREDITASI ARAS 1 STANDARDS MALAYSIA CENTURY SQUARE, LEVEL 1 & 2, BLOCK 2300, JALAN USAHAWAN, 63000 CYBERJAYA, MALAYSIA**
Pengerusi	**:**	**Y.Brs. Dr. Amirudin bin Abdul Wahab Setiausaha Bahagian Dasar ICT**
Agenda	**:**	**Lampiran 3**

3. Sukacita dimaklumkan, pihak Tuan/Puan adalah dijemput untuk menghadiri bengkel tersebut. Kerjasama adalah diminta untuk memaklumkan kehadiran dengan menggunakan borang di Lampiran 4 yang disertakan pada atau sebelum XX April 2010 (Hari). Seorang pegawai kanan–yang

bertanggunjawab dalam pelaksanaan dasar dan seorang pengurus IT di kementerian masing-masing

4. Sebagaimana pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan sedia maklum, Mesyuarat Jemaah Menteri pada 24 Februari 2010 telah memutuskan bahawa:

a) Supaya dilaksanakan Pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (Information Security Management System-ISMS) untuk sektor-sektor Prasarana Maklumat Kritikal Negara (Critical National Information Infrastructure - CNII);

b) Supaya pelaksanaan Pensijilan ISMS ini diselaraskan oleh kementerian-kementerian dan agensi-agensi regulatori yang bertanggungjawab terhadap sektor CNII Negara; dan

c) Supaya organisasi-organisasi CNII mendapat Pensijilan ISMS dalam tempoh 3 tahun.

5. Keputusan ini adalah salah satu langkah penting dalam pelaksanaan Dasar Keselamatan Siber Nasional (*National Cyber Security Policy* - NCSP) yang antara lain, bertujuan mempertingkatkan keselamatan CNII, yang mana sekiranya berlaku pencerobohan, kemusnahan atau kerosakan, akan menyebabkan kerugian yang amat besar kepada ekonomi, pertahanan negara atau menjejaskan fungsi kerajaan dan imej Negara.

6. Bagi memudahkan perbincangan sesi begkel yang akan diadakan, sukacita sekiranya pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan dapat :

a) Mengenalpasti organisasi-organisasi CNII dibawah kawalan atau pemantauan pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan yang wajib mematuhi keputusan Jemaah Menteri seperti di Perenggan 2;

   i. Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan diminta untuk menyediakan satu senarai organisasi dibawah kawalselia bagi tujuan tersebut

b) Memantau pematuhan kepada keputusan Jemaah Menteri tersebut; dan

c) Melaporkan status pematuhan dari semasa ke semasa ke:

   i. Jawatankuasa Penyelaras Keselamatan Siber Nasional (*National Cyber Security Coordination Committee* - NC3) yang dipengerusikan oleh Y.Bhg. Dato' KSU MOSTI; dan

   ii. Jawatankuasa Penasihat Keselamatan Siber Nasional (*National Cyber Security Advisory Committee* - NaCSAC) yang dipengerusikan oleh Y.Bhg. Tan Sri KSN.

7. Sebagai langkah awal, semua organisasi yang telah dikenalpasti sebagai CNII adalah dikehendaki mendokumenkan skop pelaksanaan dan pensijilan ISMS yang dirancang dan melaporkannya kepada NC3 melalui pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan.

8. Sebagai rujukan, dilampirkan bersama ini beberapa garis panduan supaya penguatkuasaan dan pemantauan kepada keputusan Jemaah Menteri ini mencapai objektifnya:

a) **LAMPIRAN 1: Panduan mengenalpasti organisasi CNII dan pemantauan pematuhan arahan jemaah menteri berkaitan pelaksanaan dan pensijilan ISMS.**

b) **LAMPIRAN 2: Contoh arahan kepada organisasi CNII berkaitan pelaksanaan dan pensijilan ISMS**

9. Sehubungan itu, pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan adalah diminta membuat persediaan untuk memberi khidmat nasihat dan panduan kepada organisasi-organisasi CNII di bawah kawalselia pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan dalam menentukan skop-skop yang bersesuaian untuk pensijlan ISMS.

10. Segala pertanyaan berkaitan perkara ini boleh dirujuk kepada <pegawai berkenaan>.

11. Kerjasama pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan berhubung dengan perkara ini didahului dengan ucapan terima kasih.

"BERKHIDMAT UNTUK NEGARA"
MALAYSIA INOVATIF, MERAIKAN KREATIVITI

(xxxxxxx)
b.p. Ketua Setiausaha
Kementerian Sains, Teknologi dan Inovasi

LAMPIRAN 1

PANDUAN MENGENALPASTI ORGANISASI CNII DAN PEMANTAUAN PEMATUHAN ARAHAN JEMAAH MENTERI BERKAITAN PELAKSANAAN DAN PENSIJILAN ISMS

Introduction

1. The National Cyber Security Policy (**NCSP**) requires the CNIIs to implement adequate security measures to ensure that the delivery of their critical services and products are not disrupted because of problems with the information assets and information systems that are used to manage, control or deliver such services and products.

2. The Definitions and Terminologies section that follows contains an explanation or elaboration of some commonly used terms and acronyms. The proper understanding of these terms will enable the right perspective pertaining to what is required and what is not. All parties are strongly recommended to read and understand these definitions and terminologies to ensure that they focus their resources on the correct issues to comply with the *Jemaah Menteri's* decision, and not waste efforts on other areas, thinking that these other areas contribute to the compliance to the *Jemaah Menteri's* decision.

3. The following section builds on the definition and terminologies to refine the discussions and clarifications that should assist all parties to have a better understanding in implementing the *Jemaah Menteri's* decision.

Definitions and Terminologies

4. **Availability**: Clause 3.2 of MS ISO/IEC 27001:2007 defines availability as "the property of being accessible and usable upon demand by an authorized entity".

   In the context of this document, availability refers to: the property or state of a subject being available for use. See *Information Availability and Service or Product Availability*. Care must be taken when discussing or mentioning the term Availability, i.e. whether the issue is about Information Availability or, Service or Product Availability, unless the Information content is the service or product. See *Information Availability* and *Service or Product Availability.*

5. **CNII**[1]**:** Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on:

   a) **National economic strength** - Confidence that the nation's key growth area can successfully compete in the global market while maintaining favourable standards of living.

[1] Source : National IT Council Portal - http://www.nitc.org.my/index.cfm?&menuid=60

b) **National image** - Projection of the national image towards enhancing stature and sphere of influence.

c) **National defense and security** - Guarantee sovereignty and independence whilst maintaining internal security.

d) **Government capability to function** - Maintain order to perform and deliver minimum essential public services.

e) **Public health and safety** - Delivering and managing optimal health care to the citizen.

The CNII entities are those that depend on information assets or information systems for the delivery of their Critical Services or Products to the nation.

6. **Critical Services or Products**: Within the context of the NCSP, the Critical Services or Products are those that are delivered to the external organisation or the organisation's consumers and satisfy the critical services or products availability needs of the external organisation or consumers i.e. industry, public, the economy and the nation. This external organization or consumers may be other CNII entities.

   However intra-services or products, i.e. services from one department that serves other departments in the same organisation e.g. Human Resources, Procurement and Finance, are NOT considered critical from the NCSP standpoint UNLESS those intra-services or products contributes to the immediate availability of the critical services or products delivered to the external organisation.

7. **Cyber Security**: Merriam-Webster defines cyber security as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (http://www.merriam-webster.com/dictionary/cybersecurity)

   In the context of this document, cyber security can be understood as: The security of information that exists in digital form. This comprises the Confidentiality, Integrity and Availability. Thus cyber security is a subset of information security. See *Information Security*.

8. **Governing Agencies**: These are Regulatory Bodies (see *Regulatory Bodies*), *Central Agencies*, State Agencies and Ministries that have authority to direct CNIIs under their purview to comply to government directives and decisions. Examples of these are the Prime Minister's Department that oversees Petronas and the Ministry of Domestic Trade, Cooperatives and Consumerism that oversees Bank Rakyat. The term Governing Agencies will be generally used instead of Regulatory Bodies which is specific to only one category of Governing Agencies.

9. **Information**: Merriam-Webster defines information as "(1) the communication or reception of knowledge or intelligence; (2) knowledge obtained from investigation, study, or instruction; (3) the attribute inherent in and communicated by one of two or more alternative sequences or arrangements of something (as nucleotides in DNA or binary digits in a computer program) that produce specific effects ; (4) a signal or character (as in a communication system or computer) representing data" (http://www.merriam-webster.com/dictionary/information)

According to ISO/IEC 27001, information can be furthered defined as:

Information asset - knowledge or data that has value to the organization

Information Security - preservation of confidentiality, integrity and availability of information

In the context of this document, information can be defined as: A collection of data in whatever form (digital or non digital), organized or structured in some manner that can be of use and makes sense to an organisation or a person or an equipment. This is irrespective whether the form (digital or non-digital) it is produced or transmitted or exists is understandable or not. Thus information comprising bits and bytes that flow between machines or equipment (e.g. control equipment) may not be easily understood to an intruder for example (and may not have commercial value) but the disruption (availability) or corruption (integrity), of the bits and bytes may cause equipment to function improperly or abnormally impacting the availability or quality of the services or products that the machines or equipment control or deliver.

10. **Information Availability**: The property of information being available for its intended use or purpose. Availability is one of the elements in information security, the other two being Information Integrity and Information Confidentiality. The three are commonly referred as Confidentiality, Integrity, Availability or simply CIA. See *Availability* and *Service or Product Availability*.

11. **Information Security**: Clause 3.4 of MS ISO/IEC 27001:2007 defines information security as 'preservation of confidentiality, integrity and availability of information; in addition other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

12. **Information Security Management System**: Abbreviated as ISMS, this is the management system based on MS ISO/IEC 27001 standard. Clause 3.7 of MS ISO/IEC 27001:2007 defines ISMS as that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
NOTE - The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

13. **NaCSAC:** Acronym for the National Cyber Security Advisory Committee, a committee formed under the NCSP and is chaired by the Chief Secretary to the Government.

14. **NC3:** Acronym for the National Cyber Security Coordination Committee, a committee formed under the NCSP that is chaired by the Secretary General of the Ministry of Science, Technology and Innovation (MOSTI).

15. **Regulatory Bodies**: These are agencies that have regulatory functions backed by an Act of Parliament and are one category of the Governing Agencies.

16. **Service or Product Availability**: The property of a service or product being available to serve its intended purpose. This must be distinguished from Information Availability which is an element of Information Security (unless Information is the service or product). It is possible that a service or product is unavailable because of compromises in Information Confidentiality AND/OR Availability AND/OR Information Integrity. As an example a bank's ICT systems may be working fine, but a staff in the bank has breached or compromised the confidentiality of customer information due to some weakness in controls (for example) but not technology, resulting in the Bank Negara Malaysia instructing the bank to temporarily suspend service availability while investigations, root cause analysis and corrective measures are put in place. Thus service availability is affected due

to an information confidentiality breach incident but not due to Information Availability or more specifically, ICT systems availability. See *Availability* and *Information Availability*.

Expected Questions and Clarification

17. Several questions may arise among the Governing Agencies as well as the CNII entities pertaining to the applicability of the *Jemaah Menteri's* decision and the administrative arrangements to comply with the decision. Some of the expected common questions are:

    a) Is my organisation a CNII entity?

    b) What is the difference between Adopting, Complying and Certified ISMS?

    c) What scope of the organisation's ISMS implementation needs to be reported to the NC3 and NaCSAC?

    d) What sorts of disruptions to services are considered critical?

    e) How do organisations report the compliance to the ISMS implementation decision?

    f) Will the Government fund the costs for ISMS implementation?

18. The following sections attempt to clarify these points.

    a) Is my organisation a CNII entity?

        i. The simplest answer is that if the services or products delivered to the public and the nation fall under the description explained as 'Critical Services or Products' above, then your entity is a CNII entity.

        ii. If your organization has been gazetted by the *Jawatankuasa Pusat Sasaran Penting* as a Key Point (*Sasaran Penting*) and the organization depends on ICT to deliver the critical products and services to the nation, your organization is by default a CNII.

        iii. Entities are expected to exercise good Corporate Responsibility and Corporate Governance to ensure that it is always in compliance to the intents of the government for the betterment of the nation and the public.

        iv. There are various other ways to determine whether an entity's services or products are critical or not. One test or indicator is when the public asks some key questions pointing to the adequacy or otherwise of the government policies and enforcement, following a major disruption of critical services. The questions may be as follows;

            A. Did the <u>government</u> enforce on this service provider to ensure that they provide continuous service?

            B. Do the service provider and the <u>government</u> know the extent of the commercial loss to business and industries with this major interruption?

b) What is the difference between Adopting, Complying and Certified ISMS?

   i. The terms adoption, compliance and certification or certified has occasionally been used interchangeably and warrants clarification in order to ensure that all the parties involved have the same understanding.

   ii. If an organisation claims that it is 'Adopting ISMS' it is merely a statement of intent that the organisation expresses. It does not necessarily mean that the organisation has actually implemented ISMS or in the process of implementing ISMS.

   iii. If an organisation claims that it is 'Complying to ISMS', it is a statement of claim that it is adopting and has implemented ISMS. It does not necessarily mean that its implementation is 'really' in compliance as verified by an independent party.

   iv. If an organisation claims to have been 'Certified ISMS', it means that an accredited certifying body has independently certified the organisation's ISMS implementation to the satisfaction of the standard.

   v. All involved should ensure that they understand the correct position of an organisation when it uses such statements mentioned above in their claims.

c) What scope of the organisation's ISMS implement needs to be reported to the NCSP implementation committees?

   i. An organisation may implement one or more ISMS covering different scopes. These ISMS may be implemented concurrently or in sequence and some of the deliverable documents may be applicable across ISMS boundaries.

   ii. In brief, the scope of ISMS and the progress of the ISMS implementation that must be reported to the NCSP committees are those that cover the delivery of the critical services and products. The ISMS implementation that DO NOT cover the critical services and products can be reported for statistical purposes on overall ISMS related activities, but will NOT be counted as one of those complying to the *Jemaah Menteri's* decision.

d) What sorts of disruptions to services are considered critical?

   i. Disruptions to services and products are considered critical within the NCSP context when one or more of the following criteria are met:

      A. The interruption is immediate and not gradual or deferred or delayed,

      B. The services performance level deteriorates significantly from the norm,

      C. The quality of service deviates from the normal or acceptable quality of services ,

      D. The impact of the disruption or compromise has significant and noticeable effect to industry or commerce, government operations, image, safety or defense.

ii. The above are general points to assist Governing Agencies and CNII entities to ensure proper focus of their efforts. It is by no means exhaustive and Governing Agencies may want to come up with their own elaboration of the critical disruptions to the services or compromise to information, relevant to their industry.

e) How do organisations report compliance to the ISMS implementation decision?

i. **Reporting**: All CNII entities or organisations will report their progress of ISMS implementation to their respective Governing Agencies, who will then report this to the NC3 and NaCSAC committees.

ii. **Verification**: In terms of verification,

A. for CNIIs gazetted as Sasaran Penting, CGSO's Tim Naziran will check on the validity of the reports as well as the actual implementation of ISMS, and

B. for CNIIs identified but not gazetted as Sasaran Penting, the Regulators shall request the CNIIs under their purview to provide regular progress reports on ISMS certification.

iii. **Enforcement**: Governing Agencies therefore have the responsibility to ensure both proper enforcement and accurate reporting on the ISMS implementation by the CNII entities under their purview, as they will be answerable to any questions related to the matter in NC3 or NaCSAC meetings.

f) Will the Government fund the costs for ISMS implementation?

i. ISMS implementation is similar to the Quality Management System (QMS) in many respects. Essentially it is aimed to benefit the organisation in its operations. Both the **management** systems (ISMS and QMS) will result in a verified and auditable process that will give an assurance to the Management of the organisation that the appropriate policies, procedures and controls are in place.

ii. In line with good Corporate Governance therefore, it is expected that the entity will take the necessary steps to ensure that ISMS is in place for the good of the organisation.

iii. The Government has no plans currently to fund the costs for ISMS implementation as this is seen as part of the respective entities' Corporate Governance and Corporate Responsibility, since the Government has given the appropriate approvals and licenses for entities to conduct their businesses and provide the services.

iv. Some Governing Agencies have provisions in existing Acts to enforce any new regulations or requirements. However entities are required to implement ISMS and not wait for Governing Agencies to enforce and announce penalties for non compliance.

Unique Exceptions

19. The majority of organisations involved in the implementation of the ISMS are the Governing Agencies that enforce on CNII entities, and the CNII entities themselves that implement ISMS. There are however some Governing Agencies that are also CNII entities. Bank Negara Malaysia is one example of a Governing Agency that is also a CNII entity. Organisations in such category

must ensure that they enforce ISMS on the CNII entities under their purview as well as implement and certify ISMS in their own organisations.

Governing Agencies Guidance

20. It is expected that with the explanation in this ***LAMPIRAN 1***, Governing Agencies will have adequate guidance pertaining to the identification of CNII and the operating area within the CNII to enforce the *Jemaah Menteri's* decision.

21. ***LAMPIRAN 1*** will be used as a point of reference in NCSP to ensure that all are synchronized in their understanding on the scope and applicability of the Jemaah Menteri's decision. When necessary, this will be updated from time to time.

22. All Governing Agencies must therefore ensure that their representatives attending NC3 meetings, NaCSAC meetings or NCSP Thrust Driver meetings are versed with this guideline and the main precepts of ISMS, and are able to explain their reports or submissions when required pertaining to ISMS implementation in the entities under their purview, which may include but are not limited to the following:

    a) The inclusion (classification) or exclusion of an entity or organisation, as a CNII entity,

    b) The Critical Services or Products delivered by the entities,

    c) The rationale for the logical grouping or boundary of ISMS scopes of the entities, especially if more than one ISMS is being implemented in a particular entity,

    d) The entities' stage of progress in implementing ISMS and be ISMS certified, and reasons for deviations, if any.

Key Performance Indicators

23. All Governing Agencies will have to develop KPI's to measure the state of progress of the ISMS implementation in the entities under their purview. The KPI's should broadly cover the Plan-Do-Check-Act cycle in ISMS implementation.

Note: This section will be developed further where necessary.

LAMPIRAN 2

CONTOH ARAHAN KEPADA ORGANISASI CNII BERKAITAN PELAKSANAAN DAN PENSIJILAN ISMS

Rujukan Kami :

Tarikh:

SEPERTI SENARAI EDARAN

Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan,

PELAKSANAAN MS ISO/IEC 27001:2007 PENGURUSAN SISTEM KESELAMATAN MAKLUMAT (*INFORMATION SECURITY MANAGEMENT SYSTEM* - ISMS) UNTUK SEKTOR-SEKTOR PRASARANA MAKLUMAT KRITIKAL NEGARA (*CRITICAL NATIONAL INFORMATION INFRASTRUCTURE*-CNII)

Adalah saya dengan segala hormatnya merujuk perkara diatas.

2. Mesyuarat Jemaah Menteri pada 24 Februari 2010 telah memutuskan bahawa:

a) Supaya dilaksanakan Pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (*Information Security Management System* - ISMS) untuk sektor-sektor Prasarana Maklumat Kritikal Negara (*Critical National Information Infrastructure* - CNII);

b) Supaya pelaksanaan Pensijilan ISMS ini diselaraskan oleh kementerian-kementerian dan agensi-agensi regulatori yang bertanggungjawab terhadap sektor CNII Negara; dan

c) Supaya organisasi-organisasi CNII mendapat Pensijilan ISMS dalam tempoh 3 tahun.

3. Keputusan ini adalah salah satu langkah penting dalam pelaksanaan Dasar Keselamatan Siber Nasional (*National Cyber Security Policy* - NCSP) yang antara lain, bertujuan mempertingkatkan keselamatan CNII, dimana sekiranya berlaku pencerobohan, kemusnahan atau kerosakan, akan menyebabkan kerugian yang amat besar kepada ekonomi, pertahanan negara atau menjejaskan fungsi kerajaan dan imej negara.

4. Selaras dengan keputusan Jemaah Menteri pada 24 Februari 2010, organisasi Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan adalah diminta mengaturkan rancangan pematuhan Pensijilan ISMS sebagaimana yang telah ditetapkan oleh Jemaah Menteri. Organisasi Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan adalah dikehendaki untuk mematuhi keperluan memberi maklumbalas mengikut garispanduan yang diberi dari semasa kesemasa.

5. Sebagai langkah awal, organisasi Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan adalah diminta untuk mengenalpasti dan mendokumen skop pelaksanaan dan pensijilan ISMS yang dirancangkan dan melaporkan skop ini melalui borang seperti di **Lampiran A.** Borang maklumbalas ini hendaklah dipulangkan selewatnya pada **30 Jun 2010**.

6. Sebagai rujukan dalam penyediaan skop ISMS, **Lampiran B** mengandungi beberapa contoh skop dari beberapa organisasi lain yang telah pun memperolehi pensijilan ISMS.

7. Dengan itu, pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan adalah dinasihatkan untuk meneliti keperluan organisasi dan juga senarai perkhidmatan atau produk yang kritikal, untuk menentukan sempadan skop ISMS yang bersesuaian.

8. Proses audit dan pensijilan MS ISO/IEC 27001:2007 Sistem Pengurusan Keselamatan Maklumat - ISMS hendaklah dilaksanakan oleh badan pensijilan tempatan yang di akreditasikan oleh STANDARDS MALAYSIA

9. Segala pertanyaan berkaitan perkara ini boleh dirujuk kepada (*point of contact of the Governing Agency* ……..)

10. Untuk makluman, Standard MS ISO/IEC 27001:2007 ISMS boleh diperolehi melalui secara pesanan online di laman web www.msonline.gov.my.

11. Kerjasama pihak Y.Bhg. Tan Sri/Dato' Sri/Dato'/Datuk/Tuan/Puan berhubung dengan perkara ini didahului dengan ucapan terima kasih.

……

Senarai Lampiran:

Lampiran A : *Scope Definition Form for CNII*

Lampiran B : *Scope of ISMS – Examples From Other Organisations Certified*

LAMPIRAN A

SCOPE DEFINITION FORM FOR CNII

Note: The form in the following page must be submitted by CNII entities to their respective Governing Agencies. The ISMS Scope should be described in this form.

Guidelines:

1. The ISMS Scope should depict the intent of coverage of ISMS certification and can be refined further when the implementation is in progress. The form is used to capture the scope as it is intended by the organisation and organisations should provide a quick response and not spend too much time in finessing the wording of the scope at this stage.

2. Organisations can submit more than one ISMS Scope, each covering a specific area under an identifiable management that will be responsible and answerable over the scope defined. In fact, large organisations with several different critical services or products or cover a large geographical area are expected to submit more than one scope.

3. Planned or tentative implementation milestones are also required. This should preferably include the major activities in the implementation of ISMS broadly guided by the Plan-Do-Check-Act cycle.

ISMS SCOPE NOTIFICATION FORM

(Please use a separate form for each scope) Form NCSP-ISMS-S01

Organisation Particulars:

Name of Organisation: _____

Address: _____

_____

_____

Tel No: _____

Fax No: _____

Contact Particulars: (The contact person to answer any queries on this submission).

Contact Name: _____

Contact No: _____

Contact Email: _____

ISMS Scope:

_____

_____

_____

_____

_____

Planned ISMS Certification Date: _____

Planned/Tentative Implementation Milestones:

_____

_____

_____

Signed by: _____ **Date :** _____

Name : _____

Position: _____

LAMPIRAN B

SCOPE OF ISMS – EXAMPLES FROM OTHER ORGANISATIONS CERTIFIED

The following table in this LAMPIRAN B shows examples of Scopes of ISMS for which the respective organisations listed in the table have been certified. A more detailed list of some of the scopes for certifications publicly available can be found in http://www.iso27001certificates.com/Taxonomy/ScopeResults.asp.

Notes:

1) It should be noted that the Scope can be very brief as in examples in row 4 and 8 or it can be very elaborate and detailed as in the examples in row 2 and 10. The key guideline is that the scope must depict clearly the boundary of the ISMS coverage and should not be ambiguous to management and to the auditors.

2) Some of the Scope statements refer to a 'Statement of Applicability' or SOA document. The SOA document is one of the document artifacts in the implementation of ISMS. The SOA is not required to be submitted with the form in Lampiran A.

3) Organisations are advised to get proper guidance in the implementation of ISMS in general and in defining the Scope of ISMS, which should focus on the critical services or products within the context of the NCSP.

No.	*Organisation*	*Country*	*Organisation's ISMS Scope (for which ISMS certification has been obtained)*
1	Nation Fire Agency, Ministry of The Interior	Taiwan	The provision of development, operation and maintenance of the Emergency Management Information System, management of related server room activities and network infrastructure supporting activities which are provided by Information Office. This is in accordance with the Statement of Applicability, ISMS - SOA, Ver. 1.2, dated 2 Dec.2008
2	National Immigration Agency	Taiwan	The Information Security Management System for Managing the National Immigration Information System (Entry and Exit Application Processing and Permit Issuing System, Airport and Seaport Document Inspection System and Digitalized Documentation System) and Operations for related Offices and Server Rooms Located in Taipei Headquarters, Taoyuan and Kaohsiung Airports
3	National Internet Development Agency of Korea	Korea	The information security management system for .kr domain name service operation and management provided by Internet Address Resources Management Centre. This is in accordance with the SOA 2.0
4	National ITMX Company Limited	Thailand	Interbank Transaction Management and Exchange Services: - Bulk Payment Systems - Single Payment Systems - Back Office Systems
5	Navy Command Headquarters, Ministry of National Defense, R.O.C.	Taiwan	The provision of operation and administration of internal information systems, management of training and server rooms activities and network infrastructure supporting activities which are provided by Information Management and Warfare Section. This is in accordance with the Statement of Applicability, ISMS-SOA, Ver.1.1, dated 25 Sep. 2008.
6	National Police Agency Ministry of the Interior	Taiwan	The provision of development, operation and maintenance of information systems for E-policy Platform including case acceptance, data processing, reporting, system administration, server room activities and network infrastructure supporting activities which are provided by the Information Management Office. This is in accordance with the Statement of Applicability, ISMS-01-03, dated 15 Oct. 2007.
7	NTT Communications China Co.,Ltd.	China	Information Security Management System covering provision of total ICT (Information Communication Technology) solutions and ICT (Information Communication Technology) managed services based on global IP(Internet Protocol) network. Statement of Applicability (SOA) (SEC-07， V1.0， 2008.9.19)
8	PGE Elektrownia Turów S.A.	Poland	Electric power and heat energy production, in accordance with the latest version of the Statement of Applicability
9	Taipei Water Department	Taiwan	The provision of the business activities relating to on-line water quality data collecting, transmitting and analyzing which are provided by Water Quality Monitoring System of the Taipei Water Department. This is in accordance with the Statement of Applicability Version 3.0 dated 27 Oct. 2006

No.	*Organisation*	*Country*	*Organisation's ISMS Scope (for which ISMS certification has been obtained)*
10	Air Navigation and Weather Services, Civil Aeronautical Administration, Ministry of Transportation and Communications	Taiwan	The provision of development and maintenance of the ATCAS (Air Traffic Control Automation System) including TACCAS (Taipei Area Control Center Automation System) and TCCAS (Terminal Control Center Automation System) which are provided by the ANWS, CAA, MOTC (Air Navigation and Weather Services, Civil Aeronautics Administration, Ministry of Transportation and Communications). This is in accordance with the Statement of Applicability, I-ISMSAO103-031, Revision 3.1, 9 May 2007
11	Meat Hygiene Services	UK	The Information Security Management System relating to the provision of information assets and systems located in Foss House, York used by MHS staff and authorised users to deliver statutory meat inspection as directed by the Food Standards Agency. This is in accordance with version 2.1 of the Statement of Applicability.
12	KAOHSIUNG MUNICIPAL UNITED HOSPITAL	Taiwan	Computer room operation, backbone network, Health Information System application registration services and Health Information System database security provided by Information Management office in accordance with the Statement of Applicability, Revision 1.1