Contribution ID: **561** Type: **Interactive Content Presentation**

THRUSTWORTHINESS PERSPECTIVE IN THE INTEGRATION OF NUCLEAR COMPUTER SECURITY INTO STATE'S CYBERSECURITY REGULATION IN INDONESIA

Nowadays, Indonesia has three research reactors managed by National Nuclear Energy Agency of Indonesia (BATAN) which located in Yogyakarta, Bandung and Serpong. The reactors were not constructed based-on digital technology, therefore we are not worrying about cyber attacks. However, in the near future Indonesia plans to build a prototype of advanced small nuclear power plant. The latest technology employed in an advanced nuclear power plant usually based-on digital technology. Therefore, the problem of nuclear computer security should be considered as well.

From nuclear computer security point of view, Indonesia do not have a specific regulation on nuclear computer security. Indonesia currently has BAPETEN Chairman Regulation (BCR) no 3/2011 on the Nuclear Reactor Safety Design and BCR no 5/2011 on the Maintenance of Non Power Reactor. These BCRs has no specific item describing about nuclear computer security. Even though IAEA document NST 045 on Computer Security on Nuclear Security described that the state should develop and maintain a national computer security strategy as part of its nuclear security regime, and the state should designate a competent authority to lead responsibility in the development of the strategy.

Ministry of Communication and Information - Republic of Indonesia, as leading sector in the field of Telecommunications and Information and national information security managers and policy has the role as reference for the formulation of a national strategy road map on cyber defense. They have five cyber security policy agendas in establishing a Secure Cyber Environment, through implementation of strategy models "Ends-Ways-Means" which focus on measurable goals, priorities and actions. Based-on the strategy cyber defense must be systematically coordinated and integrated. It cannot be treated as sporadic and casuistry. Therefore, the acquisition and utilization of technology, including information technology especially in the nuclear area, should have to be able to speed up, simplify and ensure the completion of the strategic problems of the nation and the State. Up to now, cyber defense application in Indonesia still has not become a national initiative coordinated. Implementation steps remains sectoral and based on the interests and abilities of each. Capability and deterrence and prevention, and recovery were still weak, so it is still very vulnerable to attack that is massive. Several initiatives have been undertaken by agencies and corporate institutions in order to implement cyber defense that has been done such as (a) Ministry of Communication and Information established the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTI) in 2007, (b) National Code and Cyber Agency has a unit that specializes in securing ICT resources, especially with regard to Signal Intelligence.

Indonesia as a multi culture nation has hundreds of subculture which provides great effects to the nuclear security and also nuclear computer security. Culture differences and characters do not want to understand differences will be a source of suspicion and distrust between personnel in an organization. Conflict between communities with differences in for example political group will lead to destruction and riot. The destruction can occur everywhere including in nuclear computer security environment.

IAEA document NSS-13 describes that the State laws, regulations, or policies regarding personal privacy and job requirements should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a graded approach. The trustworthiness is implemented to persons with authorized access to sensitive information or, as applicable, to nuclear material or nuclear facilities

This paper describes design of nuclear computer security regulation which will be integrated to the state's cyber security regulation. The new regulation will emphasize on how to anticipate the weaknesses of thrustworthiness due to the existence of multi culture in Indonesia. Base of the regulation is the Act No.11/2008 on Information and Electronic Transactions (ITE Law) and Government Regulation No. 82/2012 on the Implementation of Electronic Transactions and Systems as foundation to build national Cyber Security and Cyber Defense Security.The regulation will be constructed sequentially in 2 steps, conceptual step and drafting step. This paper explains the regulation in the state of conceptual step. Framework of Government Regulation in Indonesia includes (a) title, (b) introduction, (c) core, (d) closing. The title is about Government Regulation on "Nuclear Computer Security to Strengthen the National Cyber Security". Introduction will discuss on background, scope, objective, benefit, structure, definition. The core includes chapters on (a) Concept and Context, (b) Roles and Responsibility of State, (c) Roles and Responsibility of Stakeholders, (d) Establishing the

State on Cyber Security, (e) Establishing the Nuclear Computer Security Strategy, (f) Establishing the Nuclear Computer Security Culture, (g) Implementation of Nuclear Computer Security, (h) Improvement of Nuclear Computer Security Plan, (i) Sustaining of Nuclear Computer Security. The closing will discuss on sanction. We hope that the Government Regulation will strengthen the nuclear computer security to protect the public and environment from the utilization of nuclear energy in Indonesia.
Keywords : trustworthiness, nuclear computer security, cyber security, regulation, Indonesia

State

Indonesia

Gender

Male

Primary author: NUGROHO, Djoko Hari (BAPETEN)

Presenter: NUGROHO, Djoko Hari (BAPETEN)

Track Classification: PP: Insider threats