Country Paper
In Cybersecurity Initiative

National Cybersecurity
Policy & Implementation
for Government of Indonesia

by
Hammam Riza – BPPT
Moedjiono – DepKominfo

Jakarta
2006

1 Status of Information and Communication Technology

1.1 Telecoms and Information Technology Background

Indonesia's political instability, volatile economy and half-hearted telecommunications deregulation have created a high-risk environment for investors, and considerably slowed the pace of progress in the telecoms sector. Indonesia had 4.3 fixed phone lines per 100 people in 2004, or just 9.7m telephone lines.
However, coverage is greater than these measures suggest, owing to 220,000 wartel (telephone kiosks). The inadequacy of fixed-line provision has led to rapid growth in mobile-phone subscriptions, which stood at 7.4m in 2004, up from 6.3m in 2003. Personal computer (PC) and Internet penetration is also low, although rising rapidly, with just 11 PCs for every 1,000 people and just 3.6 Internet users per 100 people in 2003. There are over 6,000 local companies producing computer equipment, but they are typically small in size and the large foreign players continue to play a dominant role in the market. Pirated software and computer equipment and mobile-phone counterfeits are readily available.

1.2 Demand

Indonesia has low teledensity, at an estimated 4.6 lines per 100 people in 2004. This compares with an estimated 12 lines in Thailand and 18 lines in Malaysia. There are, however, 220,000 wartel (telephone kiosks), covering even the remotest areas, which means that overall telephone coverage is far higher than the number of lines suggests. Businesses account for 19.8% of lines, households for 78.8% and the government for the remainder. An international connection service is available to only 300,000 people, or around 0.2% of the population (with business accounting for 94% of this total, households for 5.6% and the government for 0.4%). Teledensity rose sharply during the 1990s, with an increase in the number of telephone lines from 1.4m in 1992 to 4.7m in 1997. However, the 1997-98 economic crises led to the rescheduling and indefinite delay of a number of expansion projects.

Mobile-phone penetration is still relatively low in Indonesia, at around 14 phones per 100 inhabitants (2004 estimates), compared with 53 in Malaysia, but the market is growing rapidly. By end-2002 the mobile market was larger than the fixed-line market. Users are estimated to have increased from 6.6m at end-2001 to over 32m by end-2004. Of these, 40% of users are based in the greater Jakarta area. Private involvement and investment in the sector has meant that it is more competitive and dynamic than its fixed-line competitor.

There were estimated 9.3m Internet users in Indonesia at end-2004, according to Pyramid Research, a UK-based telecoms consultancy. It is estimated that well over 50% of users access the Internet via Internet cafes, while a further 40% access the Internet from the workplace. PC penetration is also growing rapidly, however, and had reached an estimated 12.8 per 1,000 people at end-2004.

In 2003 the Indonesian Association of Internet Service Providers (APJII) announced an ambitious program to bring together public and private organizations to connect more of Indonesia's secondary schools to the Internet. Two US firms, Oracle and Cisco, have taken the lead roles in this campaign.

Indonesia information technology (IT) market is one of the smallest in the Asian region, according to IDC, an IT and telecoms advisory firm. IDC reports that IT spending was US$1.4bn in 2003 and rose by 11% year on year to US$1.55bn in 2004. This compares with US$2.8bn in Malaysia and US$2.2bn in Thailand in 2004 (both much smaller countries in population terms). The commercial sector accounts for about 80% of Indonesia's IT spending, with consumer spending accounting for about 10%.

1.3 Supply of Technology

At end-2004 there were an estimated 200 software and information technology (IT) service companies in Indonesia and 6,000 hardware companies. The majority of the local companies are original equipment manufacturers (OEMs) producing personal computers (PCs) and peripherals for the local market. A number of large US, Japanese and South Korean companies such as Mitsubishi, Sharp, LG Electronics, Dell and Sony also have manufacturing facilities there. Typically, however, imports from China of computer hardware goods are cheaper than locally produced equipment.

Indonesia is a signatory to the World Trade Organization (WTO) Information Technology Agreement (ITA). The ITA is essentially a tariff-cutting mechanism, which requires developing-country signatories, including Indonesia, to remove all tariffs on IT equipment by the end of 2005. Although Indonesia is cutting tariffs in accordance with its schedule, it has at various times imposed other taxes, such as a luxury sales tax, or charges.

Software piracy is a major problem in Indonesia. The Business Software Alliances (BSA) reports that pirated software accounted for 88% of Indonesia's software market in 2002, inflicting losses estimated at US$79m on software producers (in 2003, 88%, US$158m losses; in 2004, 87%, US$183m losses; in 2005 87%, US$280m losses). The government has enacted an intellectual property rights law in an effort to tackle software piracy, but faces the more formidable tasks of swaying public opinion and enforcement. The latest effort in legalizing the use of software is the Indonesia Goes Open Source (IGOS) initiative from five ministries lead by Ministry of Research and Technology and Ministry of Information and Communication. IGOS Consortium is formed to develop, deploy and support the implementation of IGOS Desktop system in all government institutions.

The Indonesian government has promoted the rise of domestic technology firms. Major local producers include Mugen, AAC, Aldo, ACS, ICM, Ascom, DMC, Access, NET, Procom, CBM, Columbia, Hitech and Centrin. Together, Mugen, AAC, ACM, Aldo and Access represent almost 60% of the market. They supply their products primarily to small companies, government and households. However, foreign companies remain prominent suppliers of IT and telecoms equipment. Computer clone manufacturers as well as well-known firms, including Compaq (US), IBM (US), Hewlett-Packard (US) and Acer (Taiwan), operate in the market.

Investment in information and communications technology (ICT) manufacturing is booming in some parts of the country, particularly in the free-trade zones of Batam and Bintan, both of which are situated near Singapore. Foreign companies have set up production sites for radio transmission sets, fibre-optic components, cellular phone parts and electronics. In 2004 Matsushita Electric Industrial (Japan) announced that it was planning to spend about US$5m on a new computer-equipment factory, and US-based E20 Communications is to double output of fibre-optic parts from its plant in Bintan.

2 Cybersecurity Policy

The Indonesia government should set forth several priorities in order to have a national strategy for cyber security, including security response system, threat and vulnerability reduction program, security awareness and training program and security for government's cyberspace.

Based on the above aspects and examining other national security strategies as suggested in Implementing Homeland Security for Enterprise IT by Michael Erbschloe, we have devised several objectives for Indonesia's national cybersecurity policy. To meet the goals and participate in a national cyberspace security response system, the government of Indonesia should direct all government and local organization to take or be prepared to take the following steps:

- Prepare to participate in public-private architecture for responding to national-level cyberincidents. This may mean that under certain alert conditions organizations will need to report various types of activities and intrusion attempts.
- Prepare to contribute to the development of tactical and strategic analysis of cyberattacks and vulnerability assessments. This will require more detailed reporting of activities and intrusion attempts on an ongoing basis.
- Join in a shared view of the health of cyberspace with government agencies and other organizations.

- Be a recipient of information from an expanded cyber early warning network when the security response organization is coordinating crisis management activities for cyberspace security, and participate in national incident management efforts.
- Participate in the development of national public private continuity and contingency planning efforts as well as mobilization exercises to test plans.

To meet the goals in a national security policy for threat and vulnerability reduction program, the government will need to instruct any organization to take or be prepared to take the following steps:

- Assist in enhancing law enforcement's capabilities for preventing and prosecuting cyberspace attacks. This will mean reporting more incidents and filing necessary complaints to support the prosecution of perpetrators.
- Be forthwith in providing information that will contribute to national vulnerability assessments so that all organizations will better understand the potential consequences of threats and vulnerabilities.
- Deploy new and more secure protocols and routing technology in order to reduce vulnerabilities. This will require upgrading or replacing less secure technology
- Deploy and use digital control systems and supervisory control and data acquisition systems that the government has labeled as trusted or that in some other way meets government standards.
- Deploy and upgrade software that can reduce and remediate vulnerabilities. That will mean installing patches more frequently or eliminating less secure software from the product mix used by the organization.
- Help to analyze infrastructure interdependencies and improve the physical security of cybersystems and telecommunications systems to make them meet potential government standards.
- Contribute to a process that helps to prioritize national cybersecurity research and development agendas and assess and secure emerging systems.

The government of Indonesia need to endorse a national policy for security awareness and training effort, that should take into account the following steps:

- Participate in a comprehensive national awareness program to help enable businesses, the general workforce, and the general population to secure their own parts of cyberspace.
- Improve in house training and education programs to support national cybersecurity needs.
- Accept and have staff participate in private sector supported and widely recognized professional cybersecurity certifications.

The government also needs to build national policy for securing government's cyberspace, and organization should take or be prepared to take the following steps:

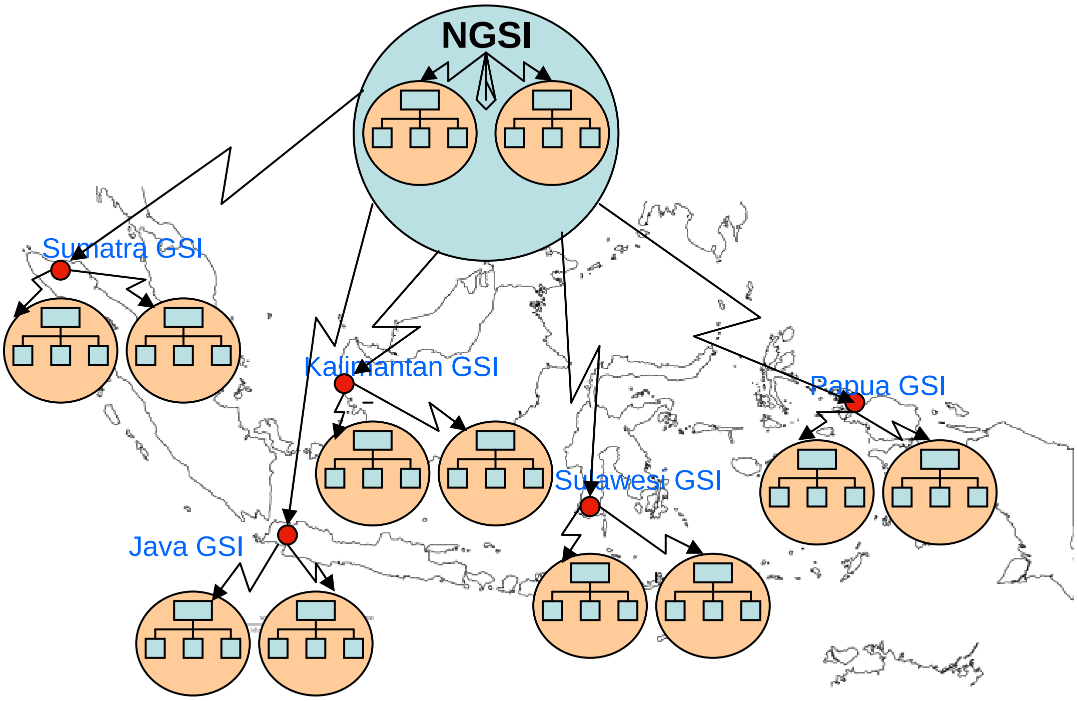
- Provide information to the government that helps to assess continuously threats and vulnerabilities to national cyber systems.
- Assure that all users in an organization that may need to use government cyber systems are trustworthy individuals and are trained on security issues.
- Provide information to government that may help to secure national wireless local area networks and keep those networks secure.
- Assist in improving security in government outsourcing and procurement by providing information as requested about contractors, equipment, software and services.
- Assist state and local government in establishing information technology security programs and encourage such entities to participate in information sharing and analysis centers with similar governments.

3 Cybersecurity Implementation for Government of Indonesia

3.1 General Overview

In order to implement the above policy, the government of Indonesia needs to form the foundation of e-government security plan by construction of government secured infra network, government data center and government data recovery center. IPTEKnet-BPPT under the Ministry of Research and Technology together with Department of Communication and Informatica is currently running a program to be funded for construction of the above secured infrastructure (as given in the diagram below). Wire and Wireless data network will be deployed for connecting between government buildings in Jakarta and fiber optic cable and transmission equipment will be installed between the government sites where the areas have a lot of the traffic volume and demand. Wireless solution will be considered to transmit the data between government buildings in same city. Government data center will be constructed for effective management of the data from each government agencies. This center will provide the various services to government agencies such as co-location, server hosting, security and backup service etc. Data backup system will secure the integrity of files and fast restoring from the fault condition.

3.2 Scope of Implementation



3.2.1 Government Secured Intra-Network and Government Internet Exchange

a. Fiber optic cable and transmission equipment

- Metropolitan fiber optic cable with 24 cores should be supplied and installed between government buildings.
- According to the installation environment of the fiber optic cable conduit, direct buried or aerial type of fiber optic cable will be used.
- Total 24 MSPP(Multi Service Provisioning Platform) with STM-16 capacity will be applied at each node where fiber optic cable will be installed. MSPP will provide various high capacity interfaces such as E1, STM-1, Fast Ethernet, Gigabit Ethernet for connection to Government Internet Exchange (GIX) operated by IPTEKnet-BPPT.

b. Wireless data solution

- In the metropolitan areas, Wireless data solution will be installed between government buildings.
- All government sites in Jakarta should be connected with wireless data solution.

c. Local area network

- Local area network will be installed at around 50 government buildings in Jakarta and government buildings in regional capital city.
- Based on the environment and number of users of each building, Wireless LAN or Ethernet network will be deployed.

3.2.2 Government Central Data Center

a. Environment of Government Central Data Center

- The floor space of data center is about 1000m^2 including operation rooms, office, equipment room and other space for power facility etc.
- UPS and rectifier with backup battery will be installed to supply AC/DC power to servers and network equipment. Power facilities must have enough capacity and consider future expansion.
- Access control and fire-fighting system must be implemented.

b. Network equipment

- High capacity backbone router and switch will be installed in government data center for internet service for government agencies.
- Backbone switches will be duplicate for the network and equipment protection
- Firewall and Intrusion detection switch will be installed in government data center for network security.
- Access switches will be installed for networking with application servers and servers of government agencies located and operated in data center.
- Modernized cabling system including UTP, fiber optic cable deployment will be applied in data center for easy cable work during any change of configuration remove of servers or network equipment.

c. Application servers

- Application servers and software such as Web server, mail server, DNS server will be installed at server farm of data center.
- Storage and related solution will be installed and the backup system can support that all application servers use the common storage disk space for effective management of data files. Backup storage will be installed in data center for providing service continuity against active

storage failure.

3.2.3 Government Data Recovery Center

a. Environment of Government Central Data Center

- The floor space of data backup center is about 500m^2 including operation room, office, equipment room and other space for power facility etc.
- UPS and rectifier with backup battery will be installed to supply AC/DC power to servers and network equipment. Power facilities must have enough capacity and consider future expansion.
- Access control and fire-fighting system must be implemented.

b. Network equipment

- High capacity router and switch will be installed in data backup center for connection to main storage in data center.
- Firewall and Intrusion detection switch will be installed in government data center for network security. Backup server will be installed for handling the data backup procedure.

4 Conclusion and Recommendation

4.1 Conclusion

a. National security policy for cyberspace of Indonesia should be written and enacted into cybersecurity laws and enforced through the application of government regulations in protecting the information assets. These policies include security response system, threat and vulnerability reduction program, security awareness and training program and security for government's cyberspace.

b. In pursuit of government objectives to develop the IT industry and promote information & communication technology with the high qualified network to be installed will increase the quality for the various government services.

c. With the efficient government infrastructure, the security of government network will be increased considerably, thus the government secured infra network will greatly contribute to the economic development due to the increased productivity and security of government organizations.

4.2 Recommendation

a. National Secured Infra-Network

- Connection between central government and government data center.
- Connection between central government and local government agencies.
- Connection between government data center and internet backbone network.

b. Government Data Management Center
    - To install backbone router and switch for connection to internet backbone network
    - To install wireless and wire-line network equipment for connection to government buildings to concentrate data traffic from government agencies.
    - To install SAN solutions for sharing files and quickly recovering data during any fails on the servers or active storages.

c. Government Data Recovery Center
    - To install backup equipment for storing the same data with government data center for emergency recovery.

d. Government Internet Exchange
    - IPTEKnet-BPPT as the government service agency is leading provider for Internet services.