Online Single Submission For Cyber Defense and Security in Indonesia

Melodia Puji Inggarwati, Berliana Dwi Arthanti, Olivia Celia

[1]Faculty of Law, Gadjah Mada University, [2]Faculty of Law, Gadjah Mada University, [3]Faculty of Law, Gadjah Mada University,

Jl. Sosio Yustisia Bulaksumur Nomor 1, Kecamatan Depok, Kabupaten Sleman, D.I.Yogyakarta 55281

Article Info: Submitted February 22, 2020 Accepted April 26, 2020 Published May 9, 2020

Vol. 4, No. 1
Month May **Year** 2020

Abstracts :

National defense and security are important issues to face the Industrial Revolution 4.0. It is undeniable that Indonesia's defense and security system's weaknesses lead to many cybercrimes. In the business licensing's sector, the Online Single Submission's (OSS) mechanism known as an important role in increasing the ease of doing business in Indonesia. The existence of the OSS system which contains a lot of important data from stakeholders that make it requires security and guarantees. But in reality, the existing OSS digital licensing system hasn't able to optimize the implementation of cyber's defense and security in Indonesia. Therefore, a breakthrough is needed to make the OSS system more perfect by integrating and guaranteeing the data through the establishment of minimum safety standards. This normative-juridical research uses secondary data that processed through literature studies and analyzed qualitatively.

Keywords: online single submission, national defense and security, industrial revolution 4.0, data security, data integration

Abstrak :

Pertahanan dan keamanan negara menjadi isu penting dalam menghadapi Revolusi Industri 4.0. Tak dapat dipungkiri bahwa lemahnya sistem pertahanan dan keamanan Indonesia mengakibatkan semakin banyaknya kejahatan siber. Dalam sektor perizinan berusaha, saat ini telah dikenal mekanisme Online Single Submission (OSS) yang berperan penting meningkatkan kemudahan berusaha di Indonesia. Keberadaan sistem OSS yang didalamnya memuat banyak data penting dari para pemangku kepentingan membuatnya membutuhkan keamanan dan jaminan didalamnya. Namun kenyataannya, sistem perizinan digital OSS yang telah ada belum mampu secara maksimal mewujudkan pertahanan dan keamanan siber di Indonesia. Maka dari itu, dibutuhkanlah terobosan baru yang menyempurnakan sistem OSS dengan mengintegrasikan dan menjamin data-data didalamnya melalui pembentukan standar minimum keamanan. Penelitian yuridis normatif ini menggunakan data sekunder yang diolah melalui studi kepustakaan dan dianalisis secara kualitatif.

Kata kunci: *online single submission, pertahanan dan keamanan negara, revolusi industri 4.0, keamanan data, integrasi data*

Citation :

Melodia Puji Inggarwati,dkk. (2020). Online Single Submission For Cyber Defense and Security in Indonesia. Lex Scientia Law Review 4(1), 89-102. doi: https://doi.org/10.15294/lesrev.v4i1.37709

1. Introduction

Indonesia is entering the Industrial Revolution Era 4.0 seems to have planned a strategy to be ready to face the Industrial Revolution 4.0 which has touched all fields. One of the government's preparations for the economy's sector is the issuance of The Presidential Regulation Number 91 of 2017 concerning the Acceleration of Business Implementation which is the effort of the government to encourage investment following the Economic Policy Package Volume 16[1]. On this regulation, an Online Single Submission System was born to accommodate the interests of business licensing's mechanisms in Indonesia, which in its implementation are so closely related to the business sector and business actors. Meanwhile, in the context of accelerating and increasing investment and business, the government declared Government Regulation Number 24 of 2018 on June 21, 2018[2].

The purpose of the Industrial Revolution 4.0 is to make things more effective and efficient following the launching of the digital licensing's system, which is the Online Single Submission's system that expected to realize a simpler and more practical licensing process that's integrated with technology so it will have a positive impact for the business investment climate in Indonesia. Now, the government has a target to improve Indonesia's ranking in the Ease of Doing Business (EoDB) index to rank 40 from previously ranked 73 in 2020[3]. Therefore, according to Edward James Sinaga, the government is currently trying to increase Indonesia's ranking in EoDB by correcting the problems on the Online Single Submission's system because one of the EoDB indicators that determined by World Bank is starting a business. If it can be realized perfectly, so the welfare of the society will be guaranteed, include increasing the comfort of investors who want to do their business activities in Indonesia because the security of their private's data has guaranteed. This can occur because of the ease given in the business licensing's procedure and the increasing ranking of Indonesia in the Ease of Doing Business which has a big influence on the business sector in Indonesia, especially in the business investment climate in Indonesia which has implications to the improvement of the economic welfare of the Indonesian people.

But unfortunately that the Online Single Submission systems in practice still found many problems, such as there are still many local regulations that overlap with The Government Regulation Number 24 of 2018 so that the data to be used is not integrated. Also, there is no synchronization data in the business location determination feature in the Online Single Submission's system results in many business locations not following regional's planning that should've been specified in the RTRW's document[4]. Because the Online Single Submission system in practice is still many problems, so it needed the synchronization between institutions related in applying for business permits is very necessary to realize a professional business licensing's scheme for stakeholders.

[1] Sony Hendra Permana. (2018). Peran Kepala Daerah Untuk Mempercepat Implementasi Paket Kebijakan Ekonomi Jilid 16. Jurnal Info Singkat, 10 (3), Pusat Penelitian Badan Keahlian DPR RI, http://berkas.dpr.go.id/puslit/files/info_singkat/, h. 2

[2] Monika Suhayati. (2018). Permasalahan Perizinan Berusaha Terintegrasi Secara Elektronik (Online Submission System). Info Singkat Kajian Singkat Terhadap Isu Faktual dan Strategis, 10 (23).

[3] Rangga Pandu Asmara Jingga. (2020). Presiden Ingin Peringkat EoDB Indonesia Masuk 40 Besar Dunia. Retrieved from https://www.antaranews.com/berita/1308510/presiden-ingin-peringkat-eodb-indonesia-masuk-40-besar-dunia. Accessed on April 15 2020

[4] Triyan Pangastuti. (2019). KPPOD Nilai Sistem OSS Masih Terkendala di Implentasi. Retrieved from https://www.beritasatu.com/nasional/574515/kppod-nilai-sistem-oss-masih-terkendala-di-implementasi. Accessed on September 28 2019

Thus, the government hopes to be able to realize data integration which also ensures the security of personal data on the Online Single Submission's system to achieving a business investment climate to improve the country's economy in the business sector. However, it is also undeniable that the presence of the business sector that has been in relation with the Industrial Revolution 4.0 seems to be an important issue for Indonesia because it is very closely related to the national defense and security on economy's sector. National defense which is an effort to maintain the sovereignty, integrity, and safety of all nations from all threats and disturbances, has a Universal State Defense System, it means that it must involve all elements of society on its implementation as referred to in article 1 paragrapgh The Act Number 3 of 2002 concerning National Defense. In the Industrial Revolution Era 4.0, Indonesia's Universal State Defense System has its own challenges, especially in preparing for cyberwar that needs cooperation from all elements of society to participate in ensuring and keeps electronic information's confidentiality, including personal data security[5]. Also, to harmonize with The Ministerial Regulation of Defense and Security Number 82 of 2014 concerning Cyber Defense, it is necessary to develop a policy/regulation of the Online Single Submission system as a foundation for its implementation in line with the realization of cyber defense in Indonesia.

One example of the data tends to be misused is the case in 2018 of Tokopedia's shareholders and company structure documents that were leaked to the public by KrAsia, a media-based in China, and it is assumed that KrAsia obtained the data from BKPM RI[6]. It shows that personal data are very vulnerable to freely accessed by irresponsible people. Moreover, if it happens as in the case of Tokopedia whose data was leaked by KrAsia, it certainly threatens the existence of personal data who incidentally the owners of data are business stakeholders in Indonesia (business actors or shareholders) which has implicated to the vulnerability of Indonesia's security and defense on the economy's sector. To avoid the same thing will happen, it's necessary to have the government's policies related to the integration of data that managed and guaranteed data confidentiality, especially in the context of the data that relates to national economic security. In accordance with this, a breakthrough in the business licensing's sector by integrating existing data in the Online Single Submission's system is considered to be a step and an appropriate strategy which following government efforts to realize Indonesia's Universal Security and Defense system to guarantee the protection of personal data.

The Online Single Submission System has been known for a long time by the Indonesian people and there have been many kinds of research that examine problems in the Online Single Submission's system, such as the effectiveness of integrated business entity registration and its relation to the hierarchy of The Government Regulation Number 24 of 2018 in statutory regulations[7], unsupported facilities (Uchaimid et al, 2019), the difficulty of internet access in a way to registration in Online Single Submission's system that occurs in some areas[8], pros and cons of The

[5] Tashia (2016). Kebijakan Keamanan dan Pertahanan Siber. Retrieved from https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber. Accessed on April 2015

[6] Mujahid Ar Razi. (2018). Dokumen Perusahaan Tokopedia Bocor ke Publik, Ini Detailnya. Retrieved from https://www.kba.one/news/dokumen-perusahaan-tokopedia-bocor-ke-publik-ini-detailnya/index.html

[7] Nurhayati, Irna., dkk (2019). Pendaftaran Badan Usaha Secara Elektronik Pasca Diterbitkannya Peraturan Pemerintah Nomor 24 Tahun 2018. Jurnal Neegara Hukum, 10(2), jurnal.dpr.go.id, h.171-172

[8] Juliani, Henny., Assegaf, M. Iqbal F., & Sa'adah, Nabitatus. (2019). Pelaksanaan Online Single Submission (OSS) dalam Rangka Percepatan Perizinan Berusaha di Dinas Penanaman Modal dan Pelayanan TERPADU Satu Pintu (DPMPTSP) Jawa Tengah. Diponegoro Law Journal, 8 (2)

Government Regulation Number 24 Tahun 2018[9], and many more. However, from the many existing kinds of research, it can be seen that there is still a lack of people who view the Online Single Submission's system more broadly by providing breakthroughs by integrating data that can strengthen and guarantee data security so it will support Indonesia's security and defense optimally, especially in the economy's sector. Therefore, the author is interested in studying further and pouring in the form of legal writing entitled "**The Role of Online Single Submission to Realize Cyber Defense and Security in Indonesia."**

PROBLEM'S IDENTIFICATION

1. How important is cyber defense and security in Indonesia?
2. What is the strategic step of data integration On the Online Single Submission to realize cyber defense and security in Indonesia?

2. Research Methods

The type of research that used in this study is normative-juridical which focused on studying the application of the rules in positive law and using the concept of positivist legis. Thus, this research used data from library materials, so it's called secondary data, which consists of primary legal material (a binding legal material), secondary legal material (such as books, journals, papers, research results from various institutions both national and international, related news, and articles), and tertiary legal material (Legal Dictionary and Large Indonesian Dictionary). Also, this research collected data by literature studies, so the data analysis uses qualitative methods which produce descriptive-analytical. Not only that, but the research approach is also carried out by observing the law and looking at the problems in society.

3. Result and Discussion

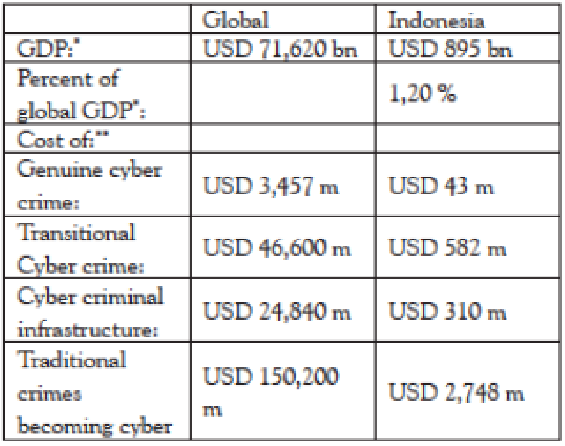
3.1 The importance of cyber defense and security in Indonesia

The Republic of Indonesia Act Number 3 of 2002 concerning National Defense states that national defense aims to safeguard and protect national sovereignty, territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of all nations from all forms of threats, both military and non-military threats. Along with the development of the industrial revolution 4.0, non-military threats, especially in the cyber space, are rife. This threat certainly does not only attack the system owned by individuals, but also the system owned by a country.

As of January to September 2019, the Badan Siber and Sandi Negara (BSSN) stated that there were around 129 million cyber attacks on Indonesia. This number will certainly increase if it is not balanced with proper handling. According to CIA data, the level of losses due to cyber crime in Indonesia is high if measured from the level of losses that occur throughout the world as shown in table 3.1.

[9] Desi Arianing (2019). Kepastian Hukum Dalam Perizinan Berusaha Terintegrasi Secara Elektronik (Online Single Submission) di Indonesia. Jurist-Diction Law Journal, 2(5)

Table 3.1. Estimated Losses Due to Cyber Crime in the world and Indonesia



	Global	Indonesia
GDP:*	USD 71,620 bn	USD 895 bn
Percent of global GDP*:		1,20 %
Cost of:**		
Genuine cyber crime:	USD 3,457 m	USD 43 m
Transitional Cyber crime:	USD 46,600 m	USD 582 m
Cyber criminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber	USD 150,200 m	USD 2,748 m

Source: *Meeting the cyber security challenge in Indonesia, an analysis of threats and responses, report from DAKA Advisory,* 2014

Based on table 3.1. It can be seen that the level of losses due to cyber crime in Indonesia has reached 1.2% of the level of losses that occur in the world. This figure is quite significant considering that various cases of cyber attacks often occur in Indonesia and even some of them attack national security and security. As an example on October 31, 2013, Indonesia was shocked by the news that Australia had tapped Indonesia through its diplomatic representative building in Jakarta[10].

Referring to data released by the International Telecommunication Union (ITU) regarding the World Siber Security Index in 2017, Indonesia is still at number 70 of other world countries. In the Asia Pacific region itself, Singapore, Malaysia and Australia rank the highest awareness of cyber security issues.

Until now, Singapore is still a role model for cyber security in the world. The country is able to implement unique and bold steps to respond to hackers and other cyber threats. In 2019, the Singapore Siberian Security Institute or CSA took a unique step, instead of rewarding the perpetrators of the hacking with punishment; they instead gave a sum of money if the hacker was able to find out what the problem was with the local government electronic system. The latest is China which has also formed cyber troops. The force was given the name "Blue Army", this force was tasked with protecting the country from cyber attacks. This digital squad will be based in the Guangzhou military region, south of China. Britain also built a cyber defense. The system, called the Cyber Security Operations Center (CSOC), is in the UK Government Communications Headquarters (GCHQ), in Cheltenham, about 160 kilometers northwest of London.

One of the factors that cause the increase in internet crime rates in Indonesia is also due to the increase in internet speed in Indonesia. According to David Belson of Akamai Research, internet speed has no connection with the large potential of

[10] Nur Khalimatus Sa'diyah . (2016). Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara. Jurnal Perspektif, 11(3)

internet crime that threatens Indonesia but hacking is more potential due to the weak internet and computer security systems in Indonesia.

In the area of licensing, in Indonesia in particular, the government has succeeded in building an integrated system that is Online Single Submission. The hard work of the government to develop this system is none other than the realization of cyber defense and security as one component of the implementation of national defense. However, seeing the reality, the government needs to reorganize a policy so that the data integrated in the Online Single Submission can be protected and not misused by other parties. In addition, the government should also equip the system with various safeguards to be free from threats that might occur in cyberspace.

3.2 *Online Single Submission* in Realizing Cyber Defense and Security in Indonesia

3.2.1 Data Security in an *Online Single Submission Online* System

The Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Transactions and Systems provides the basis for the formation of a *single online submission* system as an electronic system that functions to prepare, collect, process, analyze, store, display, announce, send and / or disseminate Electronic Information in this case in the form of company data. Data contained in the OSS mechanism is one form of electronic information used for public service purposes.

As a licensing mechanism, the OSS system plays an important role in electronic information storage. Information is a very important commodity that needs to be safeguarded [11] . OSS is in accordance with the *e-government* mechanism that has been established through The Presidential Instruction Number 3 of 2003 concerning National Policies and Strategies for *E-Government* Development. The integrated OSS system combines various data and information in one OSS container, so protecting data security is a priority. OSS Institution is an electronic system organizer based on Article 22 paragraph (1) PP No. 82 of 2012 is obliged to maintain the confidentiality, integrity, authenticity, accessibility, availability and traceability of an Electronic Information system and / or Electronic Documents. Based on that OSS Institution must strengthen the security system in OSS for the security of company data that is loaded into the system. Thus security becomes a *standard operational procedure* (SOP) in the implementation of *e-government* through OSS.

As part of one of the Electronic Systems, OSS operation permit is stipulated separately in the form of technical licensing in the field of communication and information based on Ministry of Communication and Information Regulation Number 40 of 2014 concerning Delegation of the Authority to Implement One-Stop Integrated Service in the Field of Communication and Information to the Head of the Investment Coordinating Board. The Investment Coordinating Board (BKPM) as the *Online Single Submission* Management and Implementation Institution related to Investment, whose task is to issue Business Licensing, is given the authority to issue licenses, including technical licensing in the

[11] Ardi K. Suteja, (2012). Cyber Security & Pentingnya Dunia Usaha Memahaminya : Sebuah Pengantar: Indonesia Cyber Security Forum.
International Telecommunication Union, (2018). Global Cybersecurity Index (GCI) 2018.

communication and information technology sector. Permission is a preventive juridical control as an instrument that aims to control people's behavior. Permission is issued through a series of checks on certain actions to be carried out. This check aims to find out the *costs and benefit,* the level of risk, security, and the feasibility of implementing the actions to be carried out. Permission for the OSS system shows the feasibility of implementing the OSS system in Indonesia. The preventive juridical element in the permit especially in the OSS shows that previously the OSS system has been tested from a variety of things including in relation to data security that will be integrated in the OSS system.

The Business Licensing Mechanism in OSS begins with inputting data into the system to then be issued a Business Identification Number (NIB). NIB is the identity of the Business Actor issued by the OSS Institution after the Business Actor has registered (Article 1 number 18 of the Republic of Indonesia Investment Coordinating Board Regulation Number 6 of 2018 concerning Guidelines and Procedures for Licensing and Investment Facilities). The OSS system is integrated with the Directorate General of Taxes because it deals with synchronization related to Taxpayer Identification Number (NPWP). NPWP is a number given to taxpayers as a means of tax administration that is used as a personal identification or taxpayer identity in carrying out its taxation rights and obligations (Article 1 number 20 of the Republic of Indonesia Investment Coordinating Board Regulation Number 6 of 2018 concerning Guidelines and Procedures Licensing and Investment Facilities).

In addition, the OSS system is also integrated with the Online General Law Administration (AHU Online) system of the Ministry of Law and Human Rights because it relates to the status of a business entity as a legal entity as well as with the Population and Civil Registry Office. Checking NPWP and business entity status is one of a series of initial stages of issuing business licenses in OSS. The next stages, Business Actors are required to upload several documents or fulfill requirements and / or commitments so that the status of the business license granted becomes effective.

OSS as part of the public service system has been held based on the Minister of Communication and Information Regulation Number 4 of 2016 concerning Information Security Management System. Based on Article 3 letter a of the *a quo* ministerial regulation , a government institution which is one of the state's implementing institutions as an Electronic System Operator carries out the Application of an Information Security Management System for Public Services. Under Article 1 point 6 ministerial regulation *quo* Information Security is the maintenance of secrecy (*confidentiality)*, integrity (integrity*)*, and availability (availability*)* information. Electronic System Operation is the use of the Electronic System by the state, People, Business Entity, and / or community organizers (Article 1 number 3 of the Ministry of Communication and Information Regulation Number 4 of 2016). Electronic system is a series of electronic devices and procedures whose function is to prepare, collect, process, analyze, store, display, announce, send, and / or disseminate Electronic Information (Article 1 number 1 Minister of Communication and Information Regulation Number 4 of 2016). Based on this, the OSS Institution must implement the Information Security Management System by the Electronic System Provider for Public Services based on the Risk principle as referred to in Article 2 of the *a* *quo* ministerial regulation .

Electronic Systems is a series of electronic devices and procedures in place to drill, collect, process, analyze, store, display, publish, transmit, dan.atau deploy Electronic Information (Article 1 paragraph 1 The Ministerial Regulation of Communication and Information Number 4 of 2016). Meanwhile, the strategic electronic system is an electronic system that has a serious impact on public services, the smooth running of the state, or national defense and security (Article 4 paragraph (2) of the Ministerial Regulation of Communication and Information Number 4 of 2016). OSS is part of a strategic Electronic System that has a serious impact on Public Services. The Electronic System Provider must obtain an Information Security Management System Certificate provided by the Information Security Management System Certification Agency in this case the National Accreditation Committee (KAN). KAN provides accreditation for the Information Security Management System (ISMS) Accreditation Scheme and / or Information Security Management System (SMPI). The term SMPI is used for special ISMS for organizers of electronic public service systems. KAN includes an accreditation scheme that includes one of the Information Security Management System Institutions (SNI ISO 27001) based on SNI ISO / IEC 17021-1, ISO / IEC 27006 and IAF MD. SNI ISO 27001 is a standard in the strategic Electronic System based on Article 7 paragraph (1) The Ministerial Regulation of Communication and Information Technology Number 4 of 2016. Based on Article 10 paragraph (1) The Ministerial Regulation of Communication and Information Technology Number 4 of 2016 the organizer of strategic electronic system and the operator of high electronic system must have a Management System Certificate Information Security.

Currently the OSS has been updated from V1.0 to V1.1. OSS System V.1.1. has a new feature that is increased system security (Bagus Mank Adjie in BKPM). The security of this system makes OSS an institution responsible for maintaining the security of data and information that businesses do. OSS as an integrated electronic licensing mechanism on a national scale is a breakthrough in regional licensing systems such as Surabaya Single Window in Surabaya or JAKEVO in Jakarta. This is because the OSS system is supervised directly by the Central Government. The Central Government builds, develops and operates the OSS system (Article 90 of Presidential Regulation Number 24 of 2018). Security in OSS systems is guaranteed by the OSS system integration standards as outlined in the integration-worthy certification test. The integration eligibility test certificate is stipulated by the ministry that carries out government affairs in the field of communication and informatics (Article 90 paragraph (6) of Presidential Regulation Number 24 of 2018.). The strong OSS security system and guarantees supported by supervision from the Central Government make the OSS system superior to licensing mechanisms in the regions and ministries sectorally.

3.2.2 Data Security in an *Online Single Submission* System to Achieve Cyber Defense and Security in Indonesia

Merging data in an electronic system with a strong security system is one of the efforts to realize cyber defense and security. The standard of OSS system integration based on Article 90 paragraph (3) of Presidential Regulation Number 24 of 2018 includes at least: a.) Authentication standards and regulation of access rights to and from the OSS system; b.) Standard licensing data elements between the Business Licensing system and the OSS system; c.) Standard model of integration between the Business Licensing system with the OSS system; d.) Joint security standards and digital signatures between the Business Licensing system and the OSS system; and e.) Standard *service level agreement* between the Business Licensing system and the OSS system. Meanwhile based on Article 90 paragraph (4) of Presidential Regulation Number 24 of 2018, the determination of the feasibility of standardization of OSS system integration is carried out through a process of integration due diligence, which includes a technical and operational review process on aspects which include: a.) The appropriateness of technical specifications of the application and data; b.) The appropriateness of standard operating procedures and business processes; c.) The feasibility of a permit system infrastructure standard; and d) eligibility of service support standards.

OSS has three basic principles, as follow as: 1) OSS is a national portal for managing all business licenses in Indonesia, 2) An identity that is both individuals and non-individuals must take care of NIB, 3) A permit format to facilitate investors who want to invest in any location in Indonesia (Article 1 number 17 of the Republic of Indonesia Investment Coordinating Board Regulation Number 6 of 2018 concerning Guidelines and Procedures for Investment Licensing and Facilities). Based on Article 1 number 17 of the Investment Coordinating Board Regulation Number 6 of 2018 concerning Guidelines and Procedures for Investment Licensing and Facilities, OSS is a Business Licensing issued by the OSS Institution for and on behalf of ministers, leaders, institutions, governors, or regents / mayors to Business actors through an integrated electronic system. This shows that the OSS system contains a variety of important data because it involves data from ministries, institutions, governors, or regents / mayors. The integrated OSS system which involves many licenses across Ministries, Institutions, and Regional Governments must be supported with a system security guarantee to realize cyber defense and security in Indonesia. Cyber security and cyber defense have close links, guaranteed cyber security will also guarantee strong cyber defense.

The nature of data disclosure is divided into data that is closed, limited, and open. Criteria for data and public information that are excluded are confidential and cannot be accessed by the public have been regulated in Article 17 of The Act Number 14 of 2008 concerning Public Information Openness (UU KIP) including interfering with the interests of protecting the right to intellectual property and protection from non-business partnerships healthy, data that endangers national defense and security, as well as data that reveals a person's personal secrets. Data may only be accessed by Information Users who, because of their position, duties, responsibilities and functions, have the authority to use data and information under applicable provisions (Letter h of the Definitions of Appendix to the Regulation of the Minister of Defense of the Republic of Indonesia Number 11 Concerning National Defense Information System Policy). OSS is a system that can be accessed online (in a network) or *online* using the internet. The internet is a cyberspace or *cyberspace* that can be accessed by many users. According to a survey from the Association of Indonesian Internet Service Providers (APJII) in 2017, Penetration of Internet Users in Indonesia states that there are 262 million Indonesians who use the internet which constitutes 54.68% of the entire Indonesian population. The large number of people who are connected to the internet encourages changes or transitions of crime that were originally carried out in conventional ways into unconventional ones commonly known as *cyber crime.* In July 2018, DS (18 years) succeeded in hacking the Election Supervisory Body site (Bawaslu) by testing the security or *firewall of* the Bawaslu site and stated that the government site was still weak. It don't rule out the possibility that other government information systems such as licensing systems also had the risk of hacking. The trend of the threat of cyber attacks will continue to evolve in accordance with the development of information technology, therefore, it is necessary to carry out continuous research to be able to overcome various techniques, tactics, and cyber defense strategies that will continue to develop going forward. In 1999 there were riots in cyberspace between Indonesia and Portugal over the East Timor case, even when there was a "war" with Portugal. They attacked each other until they entered the system and were able to erase all data. The threat of cyberwar or which is known as *cyberwar is* a problem that must be prevented by improving the cyber defense and security system.

Data and information security in OSS is a form of cyber security. Cyber security can be done by establishing and applying minimum security criteria for applications and software systems (International Telecommunication Union, "Global Cybersecurity Index (GCI) 2018," ITU Publications (2018), p. 7). The minimum safety criteria are reflected in the integration test certificate from the Ministry of Communication and Information that must be owned by the OSS Institution as well as the operating license of the OSS itself. In addition, Coordinating Minister for the Economy Darmin Nasution stated that the OSS system uses a cloud computing module that makes the OSS system have a large capacity storage area and a global server so that it is not vulnerable to connection failures and cannot be hacked. Minimum security criteria for applications and software systems are pillars of Legal in the Global Cybersecurity Index. The 5 (five) basic pillars of cyber security assessment based on the Global Cybersecurity Index (GCI) made by the International Telecommunication Union (ITU) are legal, technical, organizational, capicity building and cooperation (International Telecommunication Union, " Global Cybersecurity Index (GCI) 2018, " ITU Publications (2018), p.7).

The OSS data security system is also a manifestation of cyber defense to cope with cyber attacks that cause disturbances to the implementation of national defense. National defense must be carried out on various aspects. This has led to policies on the implementation of national defense carried out by other Ministries / Institutions besides the Ministry of Defense. The national defense policy is used as a reference in the implementation of national defense in accordance with their respective fields of duties and functions, that is in managing national infrastructure resources and facilities for the benefit of national defense (General Section Attachment to the Ministerial Regulation of Defense Number 19 of 2015 concerning the Policy for the Implementation of National Defense In 2015-2019). The National Task Force in accelerating the completion of Business Licensing consists of several ministers, including the Coordinating Minister for Political, Legal and Security Affairs, the Minister of Law and Human Rights, the Minister of Communication and Information and several institutions including the Head of the Indonesian National Police. The many elements involved make it clear that the essence of the Indonesian Cyber Security and Defense System is universal, so that it requires strategic and effective control, coordination and supervision of all elements of society and state officials.

The data contained in the OSS system contains information related to Business Actors that have economic value. Data must be protected in a strong system that is managed by the national center. This is because data has an important role in providing useful information for stakeholders in decision making. Data in the OSS contains requirements in the licensing stages that are important for the Government in granting business licenses. On the other hand, licensing is also important to facilitate business people in running their business. If data is lost or damaged, the licensing stage will be hampered so that it can harm various parties both the Government and business actors.

As an important commodity, data must be contained in a quality infrastructure or technology to ensure its safety. According to the Cyber Defense Guidelines , Critical infrastructure is assets, systems, and networks, which are physical and virtual, which are vital, where disruptions have the potential to threaten the security, stability of the national economy, safety and public health or a combination of them. Based on these definitions OSS is a critical infrastructure. OSS contains a lot of data on business actors, as well as licenses from the Government to provide legal certainty for those who submit licenses. Business Actors 'data must be protected because it is a human right to guarantee citizens' rights to personal protection (Considering the Bill on Personal Data Protection). The OSS system is one of the Government's efforts in realizing Cyber Defense and Security in relation to Business Actors data. Cyber Defense and Security System is a system that must be built in the midst of the current era of technological development that changes the form of information into electronic form in *cyber space* that needs to be given strict safeguards to protect the data that is in it.

4. Conclusion

Based on the discussion that has been explained before, it can be concluded that various problems or cyber attacks in Indonesia become urgency for the establishment of infrastructure or technology with an optimal level of security. National defense aims to protect national sovereignty from various threats, including non-military threats. In the era of the industrial revolution 4.0, non-military threats, especially in cyberspace, were rife to the detriment of the country. OSS is an electronically integrated system that is supervised and managed by the Central Government, has a security standard based on an integration-worthy test certificate from the Ministry of Communication and Information, uses a cloud computing module, and has obtained OSS operating license as an Electronic System. Data security in the OSS system is important to protect electronic information and to keep the licensing process smooth. Data and information security in OSS is a form of cyber security. OSS data security is also a manifestation of cyber defense to cope with cyber attacks that cause disturbances to the implementation of national defense. The OSS system exists as a manifestation of the seriousness of the government in building an integrated system and aims to realize cyber defense and security as one of the components for the implementation of national defense.

5. Acknowledgments

The author would like to thank all those who have helped in completing this writing, some of which are:

1. Faculty of Law, Gadjah Mada University, as the institution where the author is

educated;

2. Mrs. Rizky Septiana Widyaningtyas, S.H., M.Kn., as a supervisor who faithfully teaches and shares his knowledge with the author;
3. Author's parents who always provide endless support and prayers;
4. Friends Writers who always encourage; And
5. The parties that the author cannot mention one by one. Thank you for the knowledge, prayers, and support that is always given.

6. References

Books

Suteja, Ardi K., (2012). *Cyber Security & Pentingnya Dunia Usaha Memahaminya : Sebuah Pengantar*: Indonesia Cyber Security Forum.

International Telecommunication Union, (2018). *Global Cybersecurity Index (GCI) 2018.* Diterbitkan oleh ITU Publications.

Journals

Arrum, Desi Arianing (2019). Kepastian Hukum Dalam Perizinan Berusaha Terintegrasi Secara Elektronik (Online Single Submission) di Indonesia. *Jurist-Diction Law Journal, 2(5),* https://e-journal.unair.ac.id/JD/article/view/15222/8268, h. 1653

Juliani, Henny., Assegaf, M. Iqbal F., & Sa'adah, Nabitatus (2019). Pelaksanaan Online Single Submission (OSS) dalam Rangka Percepatan Perizinan Berusaha di Dinas Penanaman Modal dan Pelayanan TERPADU Satu Pintu (DPMPTSP) Jawa Tengah. *Diponegoro Law Journal, 8 (2),* https://ejournal3.undip.ac.id/index.php/dlr/article/view/24582/0, h. 1328

Nurhayati, Irna., dkk (2019). Pendaftaran Badan Usaha Secara Elektronik Pasca Diterbitkannya Peraturan Pemerintah Nomor 24 Tahun 2018. *Jurnal Neegara Hukum, 10(2),* jurnal.dpr.go.id, h.171-172

Permana, Sony Hendra., (2018). Peran Kepala Daerah Untuk Mempercepat Implementasi Paket Kebijakan Ekonomi Jilid 16. *Jurnal Info Singkat, 10 (3), Pusat Penelitian Badan Keahlian DPR RI,* http://berkas.dpr.go.id/puslit/files/info_singkat/, h. 2

Robby, Uchaimid Biridlo'i (2019). Inovasi Pelayanan Perizinan Melalui Online Single Submission (OSS): Studi Pada Izin Usaha di Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (DPMPTSP) Kabupaten Bekasi. *Jurnal Iilmiah Administrasi Publik dan Pembangunan,* 10(2), http://jurnaladministratio.fisip.unila.ac.id/index.php/administratio/article/view/98/67, h.56

Sa'diyah, Nur Khalimatus (2016). Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara. *Jurnal Perspektif, 11(3),* diakses 17 April 2020.

Sinaga, Edward James. Upaya Pemerintah Dalam Merealisasikan Kemudahan Berusaha Di Indonesia (The Government Efforts In Realizing Ease of Doing Business in Indonesia). *Jurnal Rechtsvinding Media Pembinaan Hukum Nasional 6(3).*

Suhayati, Monika (2018). Permasalahan Perizinan Berusaha Terintegrasi Secara Elektronik (Online Submission System). *Info Singkat Kajian Singkat Terhadap Isu Faktual dan Strategis, 10 (23).*

Laws and Regulations:

Peraturan Menteri Pertahanan Republik Indonesia Nomor 38 Tahun 2011 tentang Kebijakan Sistem Informasi Pertahanan Negara. Berita Negara Republik indonesia Tahun 2012 Nomor 86. Jakarta.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189. Jakarta.

Peraturan Badan Koordinasi Penanaman Modal Republik Indonesia Nomor 6 Tahun 2018 tentang Pedoman dan Tata Cara Perizinan dan Fasilitas Penanaman Modal. Berita Negara Republik indonesia Tahun 2018 Nomor 934. Jakarta.

Peraturan Pemerintah Nomor 24 Tahun 2018 tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 90. Jakarta.

Peraturan Presiden Nomor 91 Tahun 2017 tentang Percepatan Pelaksanaan Berusaha. Lembaran Negara Republik Indonesia Tahun 2017 Nomor 210. Jakarta.

Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Berita Negara Republik Indonesia Tahun 2016 Nomor 551. Jakarta.

Peraturan Menteri Komunikasi dan Informatika Nomor 40 Tahun 2014 tentang Pendelegasian Wewenang Penyelenggaraan Pelayanan Terpadu Satu Pintu Bidang Komunikasi dan Informatika Kepada Kepala Badan Koordinasi Penanaman Modal. Lembaran Negara Republik Indonesia Tahun 2014 Nomor 1947. Jakarta.

Online/*World Wide Web*

Asosiasi Penyelenggara Jasa Internet Indonesia (2017). Infografis Penetrasi dan Perilaku Pengguna Internet Indonesia: Survei 2017. Retrieved from diakses dari https://web.kominfo.go.id/sites/, Accessed on April, 17 2020

Badan Koordinasi Penanaman Modal. Perkembangan Pengembangan Sistem OSS. Retrieved from http://web.dpmptsp.jatengprov.go.id/packages/upload/portal/files/Bimtek%20Pekalongan%20Jateng%20OSS%20progres%20v11.pptx, Accessed on September 22 2019

DAKA Advisory. Meeting the cyber security challenge in Indonesia, an analysis of threats and responses. Retrieved from http://dakaadvisory.com/wp-content/uploads/DAKAIndonesia-cyber-security-2013-web-version/, Accessed on April, 17 2020

Jingga, Rangga Pandu Asmara (2020). Presiden Ingin Peringkat EoDB Indonesia Masuk 40 Besar Dunia. Retrieved from https://www.antaranews.com/berita/1308510/presiden-ingin-peringkat-eodb-indonesia-masuk-40-besar-dunia, Accessed on April 15 2020

Pangastuti, Triyan (2019). KPPOD Nilai Sistem OSS Masih Terkendala di Implentasi. Retrieved from https://www.beritasatu.com/nasional/574515/kppod-nilai-sistem-oss-masih-terkendala-di-implementasi, Accessed on September 28 2019

Razi, Mujahid Ar (2018). Dokumen Perusahaan Tokopedia Bocor ke Publik, Ini

Detailnya. Retrieved from https://www.kba.one/news/dokumen-perusahaan-tokopedia-bocor-ke-publik-ini-detailnya/index.html, Accessed on April 15 2020.

Republika.co.id. Terungkap, Lemahnya Sistem Keamanan TI Lembaga Negara. Retrieved from https://republika.co.id/berita/pbfsh409/terungkap-lemahnya-sistem-keamanan-ti-lembaga-negara, Accessed on April 17 2020.

Tashia (2016). Kebijakan Keamanan dan Pertahanan Siber. Retrieved from https://aptika.kominfo.go.id/2016/03/kebijakan-keamanan-dan-pertahanan-siber/, Accessed on April 15 2020.

Kominfo.go.id (2018). Izin Berusaha Kini Lebih Mudah, Pemerintah Meluncurkan Sistem OSS. Retrieved from https://kominfo.go.id/content/detail/13373/izin-berusaha-kini-lebih-mudahpemerintah-meluncurkan-sistem-oss/0/artikel_gpr, Accessed on September 22 2019.