The Need for Philippines Security Standards and Framework in 5G Equipment

Cybersecurity Bureau
Department of Information and Communications Technology

I. BACKGROUND

The complexity of the 5G infrastructure has introduced many cyber threats on its architecture network. It is important to understand how threat actors can manipulate the vulnerabilities and weaknesses on its assets. In addition, the increased reliance on and in the use of information and communications technology (ICT) and operational technology (OT) systems in all areas of society and, in particular, by public and private institutions that operate "Critical Information Infrastructure (CII)" in the performance of their functions have made these systems more vulnerable to various forms of cybercrimes.

New weaknesses and vulnerabilities are discovered as 5G technology is being developed and deployed. The 5G architecture considers four (4) main areas: *radio access network, core network, user equipment, and data network*. The first two (2) are considered to be significant areas of 5G Evolution. Core network operations may be performed through the cloud and other virtualization technologies. The use of open-source software poses problems with more risks that need to be addressed. Another factor is the growing vulnerabilities of Internet of Things devices that greatly expanded the number of potential entry points. Most IoT devices that are being manufactured have minimal cyber security measures. Unsecured IoT devices could easily intercept sensitive information over 5G networks. While 5G technology and standards will bring certain security improvements, threats associated with 3G and 4G will continue to impede the interoperability between previous generation networks. 5G equipment suppliers and vendors of 5G equipment must work backward to ensure adequate security.

Reports from the Philippine National Computer Emergency Response Team (CERT-PH) show the telecommunications sector is consistently among the top sectors with the most cyber incidents experienced. The election system compromise in 2016, government websites and infrastructure attacks in 2017, and the alleged telecommunications infrastructure insecurities have paved the way to strengthen the cybersecurity posture of the Philippines at the least possible time. The National Cybersecurity Plan (NCSP) 2022 of the Department of Information and Communications Technology (DICT) has created a culture of cybersecurity maturity in the country. However, programs need to be updated and sectoral support must be secured as part of the whole society's approach to cybersecurity.

The telecommunications sector, one of the identified CIIs of the Philippines, is a big target for cyber-attacks because it is the foundation of e-commerce and financial technologies, serves as the backbone for controlling and operating critical systems, and serves as the gatekeeper for the internet through the ISPs that support services essential to the nation's economy and/or government-related services. Concerns about cybersecurity and data privacy have increased due to a rise in Short Message Service (SMS)-based phishing attacks or smishing among other security threats. Hence telecom companies have intensified their cybersecurity programs to help customers protect themselves from cyberattacks

and misinformation. Following the global trends, trust in cybersecurity has become a major concern as the country is becoming more digital. This trust must be based on verifiable facts which should, in turn, be based on shared standards.

The NSCP 2022 has laid down key imperatives in the protection of the supply chain in order to address cyber insecurities while manufacturing equipment that is to be integrated into the telecommunications network and other network infrastructure of the Philippines. The protection of the telecommunications industry must be seen as a common objective and requires the combined efforts of both the public and private sectors, locally and internationally, to minimize, if not prevent, the impact of cyber-related issues. The adoption or establishment, and implementation of minimum equipment security standards and framework would lead to more efficient use of resources, improved risk management, consistent delivery of critical and essential services, effective protection of the confidentiality and privacy, the integrity of information, and availability of information that is vital to the continued functioning of our CIIs.

The study and consideration of an internationally recognized telecommunications equipment security standard are important because they provide a mechanism to validate 5G infrastructure integrity and effective cyber security. Henceforth, this paper will offer an overview of the need for a telecommunications-specific equipment security framework and a valuable reference for stakeholders, such as the operators, equipment vendors, government regulators, and application service providers allowing them to select and implement cyber-secure telecommunications infrastructure for the benefit of the Filipino people.

II. IMPORTANCE OF EQUIPMENT TESTING

Mobile networks are critical infrastructure that needs to be robust and reliable. For this reason, it is important to conduct testing on mobile network equipment and make sure that adequate security is in place. An *ICT Equipment Certification and Testing Facility* are imperative to ensure the evaluation of ICT equipment used by the CII has complied with the baseline of industry security standards. This will be anchored on the common criteria framework to determine the compliance of the manufacturer or supplier and establish guidelines to conduct benchmarking and certification. Collectively, the National Telecommunication Commission (NTC), Department of Trade and Industry (DTI), Department of Science and Technology (DOST), and other allied Philippine universities in science and technology can provide the expertise in standards, research, and development, engineering practices in testing, development, and evaluation. Ultimately, partnership with them is pivotal in the development and institutionalization of effective and efficient equipment testing programs.

To discuss further, cybersecurity standards are collections of best practices developed and published by experts to establish trust and provide a common language in protecting organizations from cyber threats and help improve their cybersecurity posture. Cybersecurity frameworks are generally applicable to all organizations, regardless of their size, industry, or sector. In the absence of testing centers, global cyber security standards and certifications can provide references and guidelines to organizations, industry, and regulators on doing a risk assessment and managing potential impact.

Several auditable international standards have been taken into consideration by DICT. Among them, ISO 27001 specifies the requirements for establishing, implementing, maintaining, and continually

improving an Information Security Management System (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.[1] ISO 27002 is the companion standard for ISO 27001. It gives guidelines for organizational information security standards and information security management practices including the selection, implementation, and management of controls taking into consideration the organization's information security risk environment(s).[2]

On the matter of 5G equipment security, the Global System for Mobile Communications (GSMA) Network Equipment Security Assurance Scheme (NESAS), jointly defined by Third Generation Partnership Program (3GPP) and GSMA, sets forth an industry-wide security assurance framework to facilitate improvements in security measures across the mobile industry. NESAS defines security requirements and an assessment framework concerning secure product development and product lifecycle processes, as well as utilizing 3GPP-defined security test cases for the security assessment of network equipment.[3]

The first aspect "security assessment of the vendor development and product lifecycle processes" requires the use of security auditors selected by GSMA to assess the process. The second aspect "security evaluation of network equipment" involves the use of security test laboratories that are ISO/IEC 17025 accredited and recognized by GSMA as being competent to evaluate products. [3]

Combined, both elements define the following approach:

- Vendors define and apply secure design, development, implementation, and product maintenance processes;
- Vendors assess their level of compliance to the GSMA-defined Vendor Development and Product Lifecycle Security Requirements;
- Vendors demonstrate these processes to external security auditors who assess compliance to the GSMA security requirements;
- Levels of security of network equipment products are evaluated and documented by security test laboratories against security requirements defined by 3GPP SA3; and
- Documentation can be forwarded to operators together with network equipment being purchased.

In this collaboration, GSMA is responsible for conducting an assessment and audit of vendors. Through organizations and agencies that specialize in security assessment and auditing, 3GPP is responsible for the formulation of security standards, assessment, and audit requirements.

NESAS development and product lifecycle assessments are done against security requirements that cover the following domains:[3]

Security by design	Security testing	Unique software release identifier

[1] ISO, ISO/IEC 27001:2013, https://www.iso.org/standard/54534.html
[2] ISO, ISO/IEC 27002:2013, https://www.iso.org/standard/54533.html
[3] GSMA, Network Equipment Security Assurance Scheme (NESAS), https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Version control systems	Vulnerability remedy independence	Security fix communication
Change tracking	Information classification and handling	Documentation accuracy
Source code review	Automated build process	Security point of contact
Continual improvement	Build process management	Source code governance
Staff education	Vulnerability information management	Security documentation
Vulnerability remedy processes	Software integrity protection	Sourcing of 3rd Party Components

Incorporating the above-mentioned to the establishment of standards will lead to a framework where the 5G telecommunication industry would have:

1. Supplier diversity
2. Interoperability
3. Fair competition
4. Adherence to the latest security standards
5. Transparency

Overall, NESAS provides a security baseline for evidence that network equipment satisfies a list of security requirements and has been developed in line with vendor development and product lifecycle processes that provide security assurance. NESAS is recommended to be used alongside other mechanisms to ensure a network is secure, in particular a suitable set of security policies covering the whole lifecycle of a network. The scheme is intended for use globally as a common baseline, on top of which individual operators or national IT security agencies may opt to put additional security requirements.[3]

The success of NESAS will work on the following parameters: (1) Network operators should require vendors to fully participate in NESAS by subjecting their processes and products to assessment and evaluation. (2) Equipment vendors should have their development and lifecycle management process assessed and their products evaluated. (3) Test laboratories should become ISO/IEC 17025 accredited, in the context of NESAS, to become eligible to undertake product evaluation. (4) ISO/IEC 17025 accreditation bodies should understand the competency requirements candidate test laboratories must demonstrate and be ready to recognize compliance.

III. EFFORTS OF DICT IN THE ADOPTION OF NESAS THROUGH WEBINARS AND CONSULTATIONS

Facilitated by DICT Cybersecurity Bureau, the first round of presentations of the Globally Recognized Cybersecurity Standards Meeting happened on 13 September 2021. NESAS was presented to a total of 64 relevant stakeholders including the telecom industry, professional associations, academe, and pertinent government regulatory organizations. Recognizing security as a driver for the adoption of standards in telecommunications, NESAS addresses baseline security issues without trying to solve

individual security problems. It defines a basic standard that a vendor can meet to show that they put the best effort into security. Implications of a failure to adopt standards for security in telecommunications were also brought up during the discussion. One of the challenges, for example, vendors will have differences in the adoption of security baselines. It will require extra work for the vendors to meet regulatory standards. It will cost them more to comply with different standards. Complexity introduces mistakes, and possibly security breaches. Having standards in place assures the adoption of necessary security controls.

The DICT Cybersecurity Bureau hosted a second meeting on 13 November 2021 and was participated by thirty-three (33) participants from the telecommunication industry both from the public and private sectors. One of the major points of discussion was the need for cybersecurity standards to be adopted and developed for equipment test facilities. Authorities on the adoption of standards in the country clarified and noted that this will lead to the promulgation of the Philippine National Standard, in which the mandated regulatory body is the DTI. Considering that the country is a signatory to the World Trade Organization, it is imperative that the Philippine government use international standards such as IEC for electronics and ITU for ICT and telecommunications. This was emphasized en banc during the discussion to clarify the dynamics of standardization. Further, it was clarified that DICT, through the Cybersecurity Bureau, is a member of the BPS Technical Committee 60 on IT and on Sub-Committee on Information Security.

Focused on the presentation and discussion of NESAS 5G Cybersecurity Framework, the third Globally Recognized Cybersecurity Standards meeting was conducted on 10 February 2022. The objective of the meeting was to hear from the industry on its stand on establishing a framework for security relative to 5G. GSMA discussed how their global association of mobile operators and mobile world congress initiated the development of standards for telecommunications. The tremendous impact of the mobile industry was underscored, around $600 Billion annual projection of 5G contribution to the global economy in 10 years and 10 Billion cellular connections worldwide, including IoT connections. The importance of supply chain security was given the emphasis on why we need security assurance: (1) mobile networks are critical infrastructures that need to be reliable and robust; (2) nation-states are beginning to regulate and restrict mobile network equipment supply; (3) security requirements are different regulations depending on which country the equipment is in, thus the uncertainty on the use of a single set of standards and performance metrics, and lastly, (4) isolated initiatives introduce complexity but do not demonstrably improve security and can introduce loopholes and weaknesses. It was emphasized that NESAS defines the baseline standard of security for different network equipment of all different vendors. The applicability of NESAS to 4G was also raised. On the side of cybersecurity, while there is a lot of consideration for 5G and its potential, DICT emphasized that there is a need to consider that 4G will continue to play a central role in markets. The NESAS Framework provides baseline security protocols that are applicable not only to 4G and 5G.

On 08 March 2022, the fourth meeting focused on the review of discussions from the past three meetings and tied together with the concerns and inputs of all stakeholders. The delineation of functions regarding standardization was clarified with the National Telecommunications Commission (NTC) as the regulatory body mandated to ensure the safety and interoperability of telecom systems while DICT is the mandated agency to ensure cybersecurity. The NESAS 5G Cybersecurity Framework was explained in detail. It is a scheme relative to the application of 5G, based on ITU IMT 2020 on interoperability. NESAS defines the baseline standards of various network equipment, regardless of the brand. These standards are technologically agnostic. GSMA is working with 3GPP, a non-government organization, which collaborates on the security requirements of Security

Assurance Specifications (SCAS). SCAS, a living document, is the specific standards upon which NESAS scheme is based. There are many versions of SCAS but the latest version is being used to complement the fast-moving standard dynamics of 5G. Test laboratories that would be adopting the NESAS Scheme should be ISO/IEC 17025 accredited. The Philippine Accreditation Bureau under DTI is the accreditation body for ISO/IEC 17025 in the Philippines.

IV. STAKEHOLDERS RESPONSE

The stakeholders' meetings facilitated by the DICT displayed positive feedback on the need to adopt minimum equipment security standards in telecommunications. Concerns raised were mostly on the process of adoption, the regulating authorities, and the mechanisms that should be established. All of which have been clarified by the DICT, NTC, and DTI-BPS. The industry is open and ready for the adoption of the equipment security standards which will be propelled by the DICT through the issuance of policies and guidelines. Lastly, the stakeholders have come to realize the importance of NESAS as an industry-led equipment security standard that would ensure cybersecurity for the Filipino people.

V. RECOMMENDATIONS AND WAY FORWARD

Various security certification schemes have been created over the last 30 years to assess the security postures of suppliers and operators and among them is NESAS, a security advancement aimed at 5G communications. It is a well-defined Globally Recognized Cybersecurity standard that raises confidence and trust in mobile network equipment.

NESAS is also a conformity scheme that includes standardization, testing, certification, and accreditation to aid in the development of a greater level of confidence and a more competitive and transparent playing field in the mobile network. In contrast to a world with various standards and diverse supply chains, cyberspace enabled by globally recognized cybersecurity standards is more likely to stimulate vigorous competition, resulting in higher quality, cheaper costs, more innovation, improved security, and increased resilience.

Based on the results of the series of stakeholders' meetings, and in line with the key imperative on the Protection of Supply Chain defined in National Cybersecurity Plan 2022 to secure the Filipino Nation, it was favorably recommended to acknowledge the importance of NESAS as one of the baselines for providing an industry-wide security assurance framework to facilitate improvements in equipment security and reliability level standards across the mobile industry leading to improving the transparency of security protection levels in the mobile industry through visual and measurable results. NESAS has been adopted in Europe and many Asian countries and continuing to gain momentum in many more places worldwide., thereby an effective way to build trust in the digital era. Why not in the Philippines?