GUIDELINES FOR CII OWNERS TO ENHANCE CYBER SECURITY FOR 5G USE CASES

Version 1.0

Cyber Security Agency of Singapore

Telecom Cybersecurity Programme Office

Contents

NOTICE

The purpose of this document is to suggest some measures to help Critical information Infrastructure Owners (CIIOs) identify the threats that can be introduced to systems when they are connected to 5G services, and to provide recommendations for mitigating cybersecurity risks. The contents herein are non-binding and meant to be informative in nature, and are not intended to exhaustively identify potential 5G threats nor exhaustively specify processes or systems that CIIOs should put in place to address or prevent such threats. CIIOs are encouraged to consider how the recommendations may be applied to their specific circumstances and to seek professional advice where required. CIIOs should exercise professional judgement if and when implementing the recommendations, and should also consider if additional measures are necessary in order to ensure cybersecurity for 5G-connected systems. This document will be reviewed and revised periodically.

This document should be read in conjunction with and does not replace, vary, or supersede any legal, regulatory, or other obligations and duties of CIIOs, including those under the Cybersecurity Act 2018, and any subsidiary legislation, codes of practice, standards of performance, or written directions issued thereunder. The use of this document and implementation of the recommendations herein also does not exempt or automatically discharge the CIIOs from any such obligations or duties. The contents of this document are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. CSA shall not be responsible for any inaccuracies, errors and/or omissions contained herein, nor for any damage or loss of any kind (including any loss of profits, business, goodwill, or reputation, and/or any special, incidental, or consequential damages) in connection with any use or reliance on this document.

1. Introduction to Singapore’s 5G Networks

In April 2020, the Info-communications Media Development Authority (IMDA) awarded the rights for Mobile Network Operators (MNOs) to build Singapore’s nationwide 5G networks using the 3.5 GHz and 28 GHz radio frequency spectrum. The rights to build 5G networks using the 2.1 GHz frequency spectrum were subsequently awarded in November 2021. The MNOs have been ramping up 5G deployment with island-wide 5G coverage expected by the end of 2025[1].

IMDA and Cyber Security Agency of Singapore (CSA) are working with the MNOs to secure the 5G networks’ deployment and operations. Singapore’s MNOs are required to ensure that their 5G networks are resilient and secure by design. This includes ensuring that the 5G networks are designed based on cybersecurity principles including Defence-in-Depth, Zero-Trust Environment and Network Element Assurance, from the outset. This collaboration will help to secure Singapore's 5G services as subscribers migrate to this next generation telecommunication platform.

Under “Defence-in-Depth”, a series of defensive mechanisms that are multi-layered with redundancies are implemented to increase security of systems and address different attack vectors. Singapore’s 5G rollout is guided by security-by-design principles with multi-layer security controls, such as distributed authentication encryption, interface authentication and security monitoring.

“Zero-Trust” means the 5G networks will not implicitly trust requests made from applications, services and users and will continuously validate all requests before granting access to its system. The outcome is a secure and trusted 5G architecture with no implicit trust in network elements, achieved through zoning & segmentation and identity & access management.

“Network Element Assurance” is fulfilled by adopting strategies based on risk management practices and achieving security assurance of the network elements through security tests, such as those described under the Network Equipment Security Assurance Scheme (NESAS). Network Element Assurance includes threat and risk analysis based on network element, secure coding, hardening, vulnerability monitoring and security testing.

Several organisations such as the 3GPP, ETSI, and IETF have worked to develop an inherently secure 5G system. Enhancements to 3GPP 5G security standards over 3G/4G services can be found in **Annex A**. However, the increased complexity of 5G networks and a shift from traditional telecommunication equipment to service-based architecture have resulted in an expanded attack surface, and therefore increased security risks to 5G network operators and users.

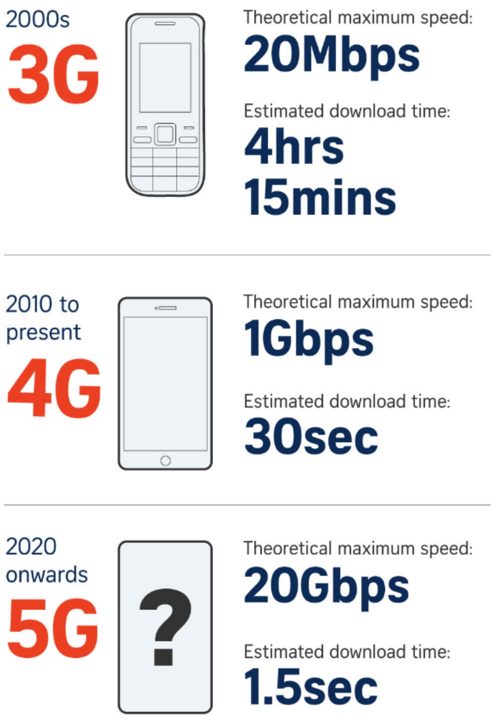
While the MNOs are required to secure their 5G infrastructure, users of 5G services are still responsible for their systems' security and be aware that connections to external networks will increase the threat surface of their systems. This document aims to help Critical information

[1] Based on IMDA’s media release titled *More Spectrum to Support 5G Growth in Singapore*, dated 26 Nov 2021.

Infrastructure Owners (CIIOs) who are users of 5G services to identify the possible 5G threats that may emerge and provide recommendations to reduce these risks. Two 5G uses cases are presented with potential threats and recommendations, to illustrate how the measures in this document can help to reduce cybersecurity risks for 5G connected systems.

What is new with 5G

The diagram below provides a comparison of the download speed (for a 4 GB file) and security aspects of the various generations of mobile technology.



3G Security:
Only has basic authentication, confidentiality & integrity protection with relatively weak encryption

4G Security:
Enhanced with symmetric-key cryptography, subscriber privacy & security protection

5G Security:
Further enhanced subscriber privacy features, stronger over-the-air encryption algorithms

Figure 1 - Comparison of mobile technologies[2]

5G promises significant enhancements over existing 3G/4G networks, such as enhanced mobile broadband (eMBB) speeds (up to 20 Gbps, a 20-fold increase over 4G's peak data rates), the ability to support massive machine-type communications (mMTC) (one million devices per km^2 – a 1,000-fold increase over 4G's capacity), and ultra-reliable low latency communications (URLLC) (less than 1ms, a 25-fold improvement over 4G's latency). These enhancements enable 5G to fulfil diverse network requirements in various scenarios. Examples of use cases include:

- Smart City and Smart Sensor Network. 5G-enabled Internet of Things (IoT) sensors can monitor air quality, energy use, traffic patterns, etc. and provide a platform for smart city solutions ranging from smart home, smart parking, to crowd management, to emergency response.

[2] Figure taken from the article by The Straits Times titled *At least two 5G networks to be rolled out by 2020*, dated 8 May 2019.

- Connected and Autonomous Private and Public Transport. Low-latency and high data-capacity 5G networks can enable roads, trains and self-driving car to communicate with each other, which facilitates safer and more efficient traffic flow.

- Smart Factories or Industry 4.0. The high reliability of 5G will enable factories to remotely control and manage their floor assets in real-time. This can enhance industry automation, reduce human risk in mission-critical situations, etc.

- Enhanced Consumer Experience. 5G users can experience high-quality broadband services anytime and anywhere, including access to immersive and interactive content with Augmented Reality and Virtual Reality.

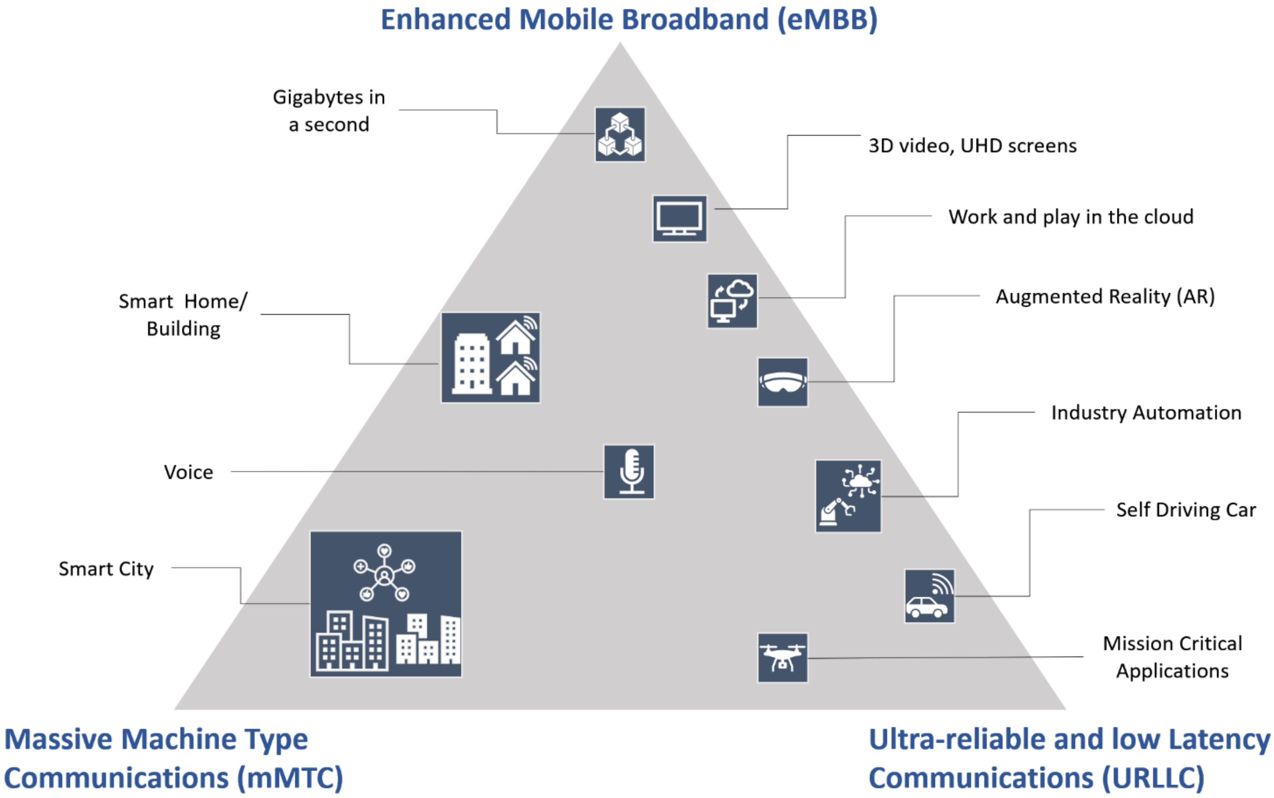

Enhanced Mobile Broadband (eMBB)
Gigabytes in a second
3D video, UHD screens
Work and play in the cloud
Augmented Reality (AR)
Smart Home/ Building
Industry Automation
Voice
Self Driving Car
Smart City
Mission Critical Applications
Massive Machine Type Communications (mMTC)
Ultra-reliable and low Latency Communications (URLLC)

Figure 2 - 5G use cases

5G Implementations

A typical 5G network consists of the **5G Core**, **Transmission infrastructure** and **Radio Access Network (RAN)**, as shown in Figure 3 below. Singapore's 5G networks are based on the Standalone (SA) architecture defined by the 3GPP. In the near term, some of our MNO deployments can be based on Non-Standalone (NSA) architecture.

- In a Standalone (SA) Implementation, the entire setup (5G Core, Transmission and 5G RAN) consists of equipment dedicated to the new 5G network. This configuration allows users to fully reap the benefits of 5G networks such as edge computing and supporting various use cases through network slicing. Depending on MNO's SA implementation, edge cloud/computing may be deployed in their networks to support ultra-low latency requirements.

- Non-Standalone (NSA) implementation leverages existing 4G Core and/or Transmission infrastructure, with new 5G RAN components added to support higher data rates. 5G RAN components include base stations (gNB) and 5G New Radio (5G NR) antenna. Most other countries are introducing 5G with NSA as the intermediate implementation before transiting to SA in the longer term.

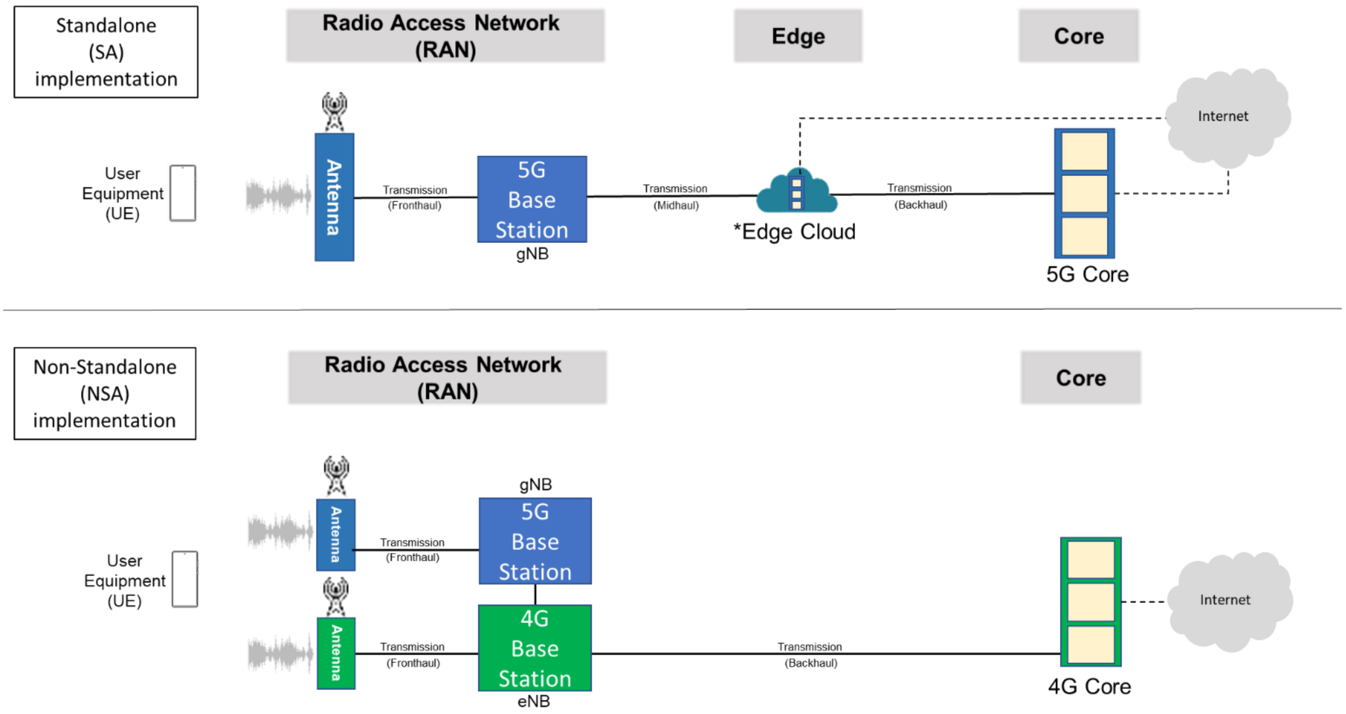


Figure 3 - Standalone 5G and Non-Standalone Implementations
**Edge Cloud is optional, depending on MNO's implementation*

There are two common spectral ranges that are utilised by 5G networks. These are the sub-6 GHz band (specifically 2.1 GHz and 3.5 GHz for Singapore) and mmWave band (28 GHz in Singapore). Table 1 summarises the differences between the two spectrums.

Spectrum	Sub 6 GHz (2.1 GHz & 3.5 GHz)	mmWave (28 GHz)
Data Rate	Up to 2 Gbps	Up to 20 Gbps
Latency	3 – 4 ms	< 1 ms
Typical Implementation	Outdoor deployment	Indoor deployment

Table 1 - Comparison of Sub 6 GHz and mmWave Spectrums

2. Purpose, Scope and Intended Audience of this Document

The purpose of this document is to suggest measures to help CIIOs identify the threats that can be introduced to systems when they are connected to 5G services provided by the MNOs and to provide recommendations for them to mitigate the cybersecurity risks of these threats. In this document, CIIOs' systems refer to systems and User Equipment (UE) owned by CIIOs and do not include Multi-access Edge Computing (MEC) and application platforms connected to MNOs' 5G infrastructure or network slices from MNOs. This document does not cover threat risk assessment of and mitigation measures for the MNOs' 5G infrastructure, network functions and applications.

The intended audience of this document includes, but not limited to, the following:

- CIIOs (e.g., senior management, communication network planners and their cybersecurity teams)
- CIIOs' service and equipment providers (e.g., outsourced ICT teams / managed security service providers / ICT equipment vendors)

3. Identifying 5G Security Threats

The cybersecurity risks for 5G systems are constantly changing with the evolution of the threat landscape and development of new application use cases. Threat actors are continually refining their techniques and procedures to launch new cyber-attack campaigns. It is important that CIIOs proactively adapt their cybersecurity policies and capabilities to protect their systems, as 5G technology is moving from traditional telecommunication protocols to IT-based protocols. Vulnerabilities which exist in IT environments are now present in 5G systems. Exacerbating the issue, new technologies such as virtualisation and cloud computing are used to enable 5G's vast benefits. These increase the attack surface of 5G networks as compared to traditional telecommunication networks.

Cybersecurity threats could also exploit indirect attack vectors, such as through victims' systems supply chain. For example, in the SolarWinds cybersecurity breach targeting victims who used SolarWinds' solutions, threat actors focused their attacks on the supplier by inserting their malicious payload into software patches they knew would be deployed in their actual target. The US Colonial Pipeline cyber-attack in May 2021 saw threat actors successfully gained entry to the network, causing grave disruption to Colonial Pipeline's operations. These show that CIIs are attractive targets to threat actors, who could be highly-skilled and well-resourced. Singapore is not immune to cyber threats and CIIs will remain as attractive targets to adversaries as shown by SingHealth incident in 2018.

CIIOs should adopt the principle of zero trust when designing their security policies, along with a defence-in-depth approach to comprehensively defend their systems. CIIOs should also continuously build up their cybersecurity capabilities and remain vigilant in securing their systems against threats. The use of a threat model will help cybersecurity defenders by providing a structured approach to categorise identified threats to their systems. Mitigation efforts to the threats can then be prioritised.

This document covers some possible threats that can be introduced when systems are connected to 5G services, using Microsoft's STRIDE threat model. The STRIDE model is a mnemonic for security threats in the following categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

While the STRIDE threat model provides a frame to categorise potential threats, the commonly used CIA triad will be used to describe the impact of cybersecurity attacks. The CIA triad is defined as:

- Confidentiality – Keeping data secure
- Integrity – Maintaining system integrity
- Availability – Preserving system services and network availability

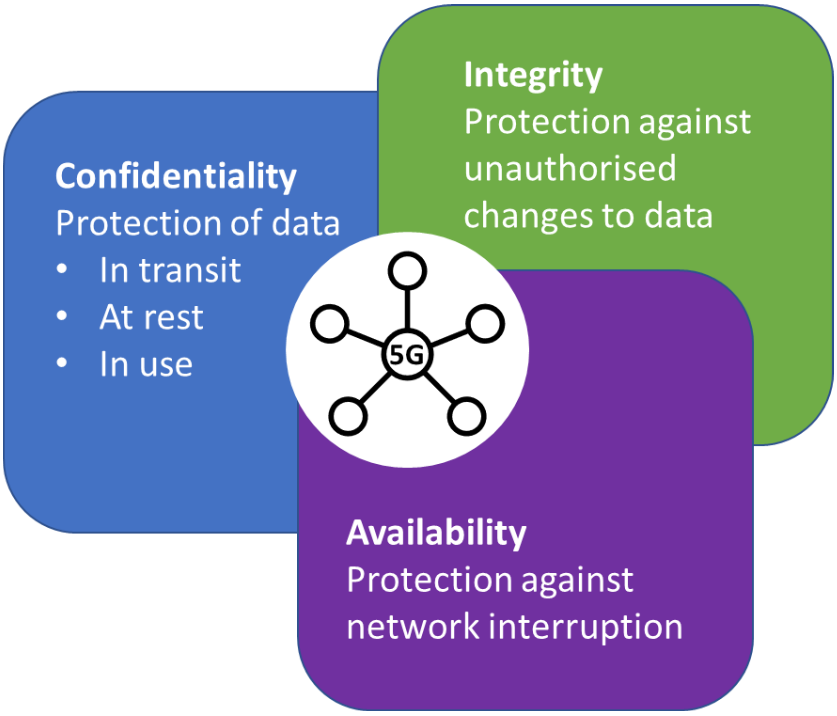

Confidentiality
Protection of data
• In transit
• At rest
• In use
Integrity
Protection against unauthorised changes to data
5G
Availability
Protection against network interruption

Figure 4 - Confidentiality, Integrity and Availability Triad

This section lists potential threats to systems connected to 5G networks based on the STRIDE model and will also map the corresponding impact of the threats to the CIA triad. The potential threats mentioned in this section are contextualised to 5G environment and readers should understand that many of these threats are not unique to 5G. Examples of potential risk scenarios are added to provide better illustration based on 5G's context.

3.1 Spoofing

Impact		
Confidentiality	Integrity	Availability

In spoofing-related threats, threat actors attempt to impersonate devices, services, or persons to carry out man-in-the-middle (MITM) attacks. The threat actor could then carry out further attacks based on the objective of their campaign.

Threat actors may attempt to spoof legitimate 5G networks or slices to deceive UE to connect to them. Threat actors may also spoof UE or its Subscriber Identity Module (SIM) to gain access to the CII network through the 5G network.

Example of a threat scenario: Threat actors identify an existing 5G network with inadequate access controls and broadcasts their own 5G signal to masquerade as a legitimate 5G network. The threat actors are then able to view the data traversing to any connected UE, compromising confidentiality and integrity. Threat actor could follow up with other malicious actions to achieve their objective of the attack campaign.

3.2 Tampering

Impact		
Confidentiality	Integrity	Availability

After threat actors have gained access to a system or network, they could attempt to make unauthorised changes to the data or network traffic to inflict damage to the system's integrity. Tampering threats could take place to the physical hardware, software, data in transit and data at rest.

Threat actors could attempt to modify the data traversing through the 5G network, such as to redirect the traffic or to change information sent. Threat actors could also physically tamper UE and its locally connected equipment, such as to connect unauthorised devices or to relocate them.

Example of a threat scenario: Threat actors physically tamper UEs by connecting to an exposed communication port, such as a USB port. Through the communication port, the threat actors can inject malware, collect sensitive data or modify settings of the UE.

3.3 Repudiation

Impact		
Confidentiality	Integrity	Availability

Repudiation in cybersecurity refers to the system or application not adopting sufficient controls to properly track users' actions or events that had occurred within a system. Repudiation threats usually aim to disrupt the auditing and tracing capabilities of system administrators and cybersecurity defenders to hide traces and evidence of a larger cyberattack. These traces and evidence are critical in the containment and investigation phases in the incident response process.

For systems which are connected to the 5G network, this could mean attacks on the UE to erase or tamper logs stored locally, or to remove the UE from network.

Example of a threat scenario: A disgruntled IT employee gains entry to application server with privileged access. Configurations are deliberately changed to cause disruptions and log entries are subsequently deleted to hide the actions.

3.4 Information Disclosure

Impact		
Confidentiality	Integrity	Availability

Information disclosure refers to data being made available to unauthorised systems or persons. The disclosure could be due to a lack of protection of the data or unauthorised traffic sniffing. The sniffing of data could also be part of the reconnaissance activities threat actors carry out to for their cyber-attack campaign. The impact would depend on the sensitivity of disclosed information and its volume. Information should be classified according to sensitivity (e.g., customers' personal data is generally sensitive due to privacy aspects). CIIs' data will be attractive to threat actors, who could target the 5G connection connected to the CIIs to gain unauthorised access to the data in transit or the data stored locally in the UE and its locally connected equipment.

Example of a threat scenario: A MITM attack is carried out by threat actors between UE and base station. Information is unencrypted before sending from UE to base station and hence can be collected in clear by the threat actors, compromising confidentiality.

3.5 Denial of Service

Impact		
Confidentiality	Integrity	[✓ Availability]

Denial of service (DoS) attacks aim to disrupt normal operating behaviour of systems and networks. The attacks could make servers and devices non-responsive or reduce the performance of networks, such as causing a reduction in bandwidth or higher latency.

With higher connectivity to machines and devices, 5G systems will be exposed to larger surface of DoS attacks. Devices connected to 5G networks would also be exposed to botnets through its Internet connection, which could carry out Distributed Denial of Service (DDoS) attacks. These attacks could cause service disruption over the 5G connection, such as lowering data rate, overloading processors of connected devices, and creating wireless interferences.

Example of a threat scenario: A threat actor broadcasts signals over the same 5G frequency spectrum to carry out DoS attacks by depleting radio resources of the nearby 5G base station and UEs. This results in unavailability of 5G services to the vicinity for systems without backup communication means.

3.6 Elevation of Privilege

Impact		
[✓ Confidentiality]	[✓ Integrity]	[✓ Availability]

In this type of threats, an adversary gains higher level of access than is authorised and modify sensitive data or change systems behaviour. Elevation of privileges usually occurs after threat actors have already gained a foothold within the system or network.

Elevation of privilege threats could occur when there are weak user access controls on the UE and its locally connected equipment. Threat actors could subsequently carry out attacks on the CII or its networks through the compromised devices.

Example of a threat scenario: Threat actor gains unauthorised access to system through brute-force attack on a user’s weak password with no multifactor authentication implemented. The threat actor carries out privilege escalation attack to achieve administrator rights and carry out unauthorised actions to modify the system’s configuration, potentially causing disruption to the entire system.

Mapping of 5G Threats to Their Impact

Table 2 maps the above threats to their impact on Confidentiality, Integrity and Availability. With the understanding of the 5G threats, the next section provides recommendations on how to mitigate them.

5G Threats	Impact		
	C	I	A
Spoofing (S)	🟧	🟧	🟧
Tampering (T)		🟧	
Repudiation (R)		🟧	
Information disclosure (I)	🟧		
Denial of Service (D)			🟧
Elevation of Privilege (E)	🟧	🟧	🟧

Table 2 - 5G Threat modelling using STRIDE model

4. 5G Security Recommendations

A system is only as secure as its weakest link. Security-by-design and defence-in-depth approaches should be adopted to ensure security is considered across the systems lifecycle, from the development stage to the maintenance stage, to allow CIIOs to tackle cybersecurity risks comprehensively.

This section provides recommendations to CIIOs intending to use 5G in their operational environment. The recommendations will focus on (1) the development & implementation, and (2) the operations & maintenance stages at which CIIOs could apply them. A checklist is provided at the end of the document (**Annex B**) to guide the CIIOs' security teams through the two stages at which the recommendations may be applied. An advantage of introducing security considerations based on different stages is to make security threats more visible and widely understood by senior management and other stakeholders. Appropriate measures may then be taken in a timely manner to reduce risk to an acceptable level.

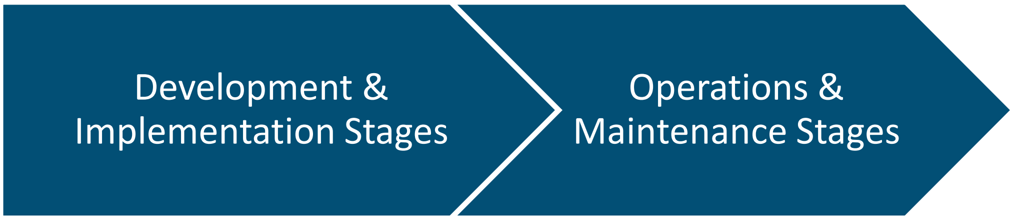

Development & Implementation Stages
Operations & Maintenance Stages

Figure 5 - Stages of lifecycle considered

While the recommendations provided in this document are focused on the 5G threats mentioned in Section 3, CIIOs will need to exercise their professional judgment to determine if these recommendations are relevant to their systems' environment.

4.1 Assurance of User Equipment

Lifecycle Stages	
🟩 Development & Implementation	Operations & Maintenance

Security assurance refers to the measure of confidence that security features, practices, procedures and architecture of an information system accurately mediates and enforces the security policy. In our context, this means the UE achieved a certain level of security assurance.

CIIOs should ensure that there are appropriate levels of security assurance for the equipment connecting their systems to the 5G network, inclusive of the UE. Equipment deployed with security assurance certifications, such as those under CSA's Cybersecurity Labelling Scheme (CLS), should maintain their certification validity throughout the deployment period.

The software and/or firmware of the equipment should be updated to minimise risks of attackers exploiting known vulnerabilities. Plans should be in place to ensure that UE which are approaching the manufacturers' End-of-Service Life period are replaced to prevent attackers from compromising the CII's network through the UE.

4.2 Segregation of Traffic

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Segregation of traffic refers to the separation of network traffic for data with different security requirements. Network traffic to the Internet for users to do web browsing would typically require less security protection than network traffic between internal servers. Proper segregation would insulate most assets from direct attacks.

The 5G network should be treated as having the same trust level as other network connection services provided by external service providers. CIIOs should consider the sensitivity of the data which would traverse through the 5G network at the planning stage and implement the appropriate policies and security solutions. Additionally, CIIOs could consider subscribing to a dedicated 5G network slice to ensure that the 5G service is able to meet its operational and security requirements.

4.3 Data Protection

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Data protection refers to the protection or safeguarding of important data from corruption, compromise, or loss. Data protection typically involves the usage of encryption to prevent unauthorised access and modification to sensitive information.

CIIOs should ensure that sensitive data is sufficiently protected during transmission. Data should be encrypted before it traverses through the 5G network. For implementations where data encryption cannot be implemented, such as in low latency use cases or where UE have low processing power, data integrity verification measures (e.g. Hashed Message Authentication Code), should be implemented. Where operationally feasible, end-to-end encryption should be implemented for all system communications.

In contracting the MNOs for their 5G services, CIIOs could require their data to be separated from other 5G subscribers, such as the use of dedicated network slices to minimise risks of unauthorised access of the data traversing through the 5G network. CIIOs could also require their 5G service provider to encrypt their traffic over the air.

Data stored locally on the UE should similarly be protected against unauthorised access and tampering, using secure industry standard algorithms with sufficient key lengths. CIIOs should determine the encryption scheme to be used for data stored locally based on the sensitivity of the data.

CIIOs could consider deploying UE which are equipped with hardware-based root of trust modules, such as the Trusted Platform Module (TPM) chip to protect critical data (e.g., authentication keys and digital certificates), against unauthorised access and tampering.

For information derived directly from the 5G service, such as the geolocation of the UE or the time, CIIOs could carry out verification of the information received with a second source where operationally feasible, such as through satellite navigation systems or an authoritative Network Time Protocol (NTP) server.

4.4 System Hardening

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Hardening reduces the risks associated with a wide range of attacks by implementing the following:

- Use of up-to-date firmware and software versions and patches
- Removal or disabling of unnecessary components
- Disabling debug settings
- Use of secure configuration options (e.g., cryptography) where supported
- Removing unnecessary default certificate authority bundles

Equipment connected to the 5G service should be hardened such that software and hardware functions that are not required cannot be activated, especially in deployments where the devices are not located within the CIIOs' premises. If unused functions cannot be removed or uninstalled individually, they should be disabled through its configuration settings. The UE should also be configured to not respond to any network requests over ports which are not used for authorised traffic. In addition, UE should be configured to only boot from authorised memory devices while in operation.

4.5 Physical Security

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Physical security refers to the protection of the facility housing system devices, the system equipment themselves, and the facilities used to support the system's operations. This refers to CIIOs' facilities or CIIOs' equipment, especially to those remotely located.

Policies for physical security measures should include UE and any equipment connected physically. Physical security controls include:

a. Physical access control with monitoring and alert capabilities to protect UE and their locally connected components should be implemented where operationally feasible, with access to be granted only to authorised personnel; and
b. Tamperproof enclosure boxes should be used where operationally feasible to protect the ports and interfaces of all equipment within the infrastructure that is connecting to the 5G network against unauthorised connection and tampering.

CIIOs could also consider protecting their equipment connected to the 5G network against potential side-channel attacks using electromagnetic (EM) emissions, and interception of coupled and directly conducted compromising emanations. EM shielding could be implemented to prevent stray emanations, along with protection against modifications to the power source.

4.6 Business Continuity Planning

Lifecycle Stages	
🟩 Development & Implementation	Operations & Maintenance

Business continuity planning refers to documented procedures that guide organisations to respond, recover, resume and restore business operations to a pre-defined level of operation following disruption and cover the resources, services and activities require to ensure the continuity of services.

CIIs and other supporting systems' dependency on the 5G network should be studied and documented with regular reviews. Contingency plans should be in place for scenarios where 5G connectivity is disrupted or compromised, with clear steps and procedures on response to common threats, triggers for activation and steps for recovery. The CIIOs should make provisions for the CII to operate in a degraded mode if the 5G connection is unavailable or compromised, such as falling back to other wireless connection (e.g., 4G or WiFi) or wired solutions, where operationally feasible.

4.7 Awareness of 5G Threats

Lifecycle Stages	
🟩 Development & Implementation	🟩 Operations & Maintenance

CIIOs should be aware of threats to their systems that are introduced due to 5G connectivity. Plans should be regularly reviewed and implemented based on industry best practices to mitigate cyber threats based on the threat landscape of the CIIO's sector.

Adequate training, including periodic review of 5G technology and threats, should be provided to educate system operators and maintenance staff managing the systems connected to the 5G network. CIIOs should conduct threat modelling for their systems and to update them regularly based on the threats to the technologies being deployed, such as 5G.

4.8 Support Requirements from 5G Service Providers

Lifecycle Stages	
🟩 Development & Implementation	🟩 Operations & Maintenance

5G service providers refer to the MNOs providing the 5G connections as well as any vendors who provide and support the UE. Expectations and requirements from the 5G service providers should be discussed and agreed upon before services are procured, stating the response times, roles and responsibilities during security incidents, as well as the escalation process for security incidents as part of the Service Level Agreement (SLA). Quality of Service (QoS), guaranteed uptime and mean time to service recovery should also be stated clearly.

A single point of contact from each 5G service provider should be provided and documented in the CIIOs' recovery and response plans. 5G service providers should also assist in the security incident investigation process, such as to store and provide related system logs. CIIOs should also be informed if there are cyber-attacks to the 5G service providers' own systems, that may lead to compromise of information relating to the CIIO.

4.9 Configuration Management

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Configuration management refers to a comprehensive description of roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems.

CIIOs should ensure that the configuration of the systems connected to the 5G network are planned, documented, reviewed and tested before implementation and throughout its operations period. Technical solutions could be implemented to document and maintain the configurations rolled out throughout the deployment period of the equipment to facilitate system recovery and prevent any accidental misconfigurations.

UE and their locally connected equipment may be deployed over a large area and may not have direct connections to the CII network. CIIOs should still ensure consistency with the latest cybersecurity policies, regardless of whether the UE have direct connections to the CII network, or how far they are located.

4.10 Access Control

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Access control refers to allowing access based on user's credentials and security posture of the UE. It includes network access control, identity and access management and interface authentication.

Technical controls should be implemented to prevent unauthorised devices or devices which no longer meet the cyber security posture from connecting to the CII network.

Access control policies could be based on the identity of the UE and access control mechanisms should be reviewed when needed. Remote access to critical assets by a third party should be minimised and subjected to strict access control, including state-of-the-art authentication, authorisation, and auditing control, especially for privileged accounts.

Access control polices for the UE could use a combination of the devices' hardware identifiers (e.g., serial numbers or International Mobile Equipment Identity (IMEI)), administrator assigned identifiers (e.g., device hostname) and SIM identity as their identity during the authentication process. Multifactor authentication is recommended to be used to authenticate users accessing the UE or making connections to the CII network through 5G.

CIIOs should select the appropriate mechanisms and authentication processes for UE based on the type of access requested and the sensitivity of the data being exchanged over the 5G network.

4.11 Asset Management

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Asset management refers to managing assets that an organisation possesses, and their status. This information provides the visibility into license utilization, software support cost, unauthorized devices, vulnerabilities, and compliance.

CIIOs should ensure that all their equipment connected to the 5G network are documented as part of their asset management process. The details of the equipment to be included in the documentation could include serial numbers, SIM, firmware version and geolocation data. The asset management systems could be integrated to the centralised monitoring system to inform of any discrepancies, such as devices using outdated firmware, or unauthorised relocation of the UE. Technical controls, such as configuration of the UE to use only whitelisted 5G SIMs, could also be used to prevent unauthorised swapping of the SIM for the UE.

4.12 Overload Controls

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Systems should be designed to handle overload conditions in a controlled rather than unpredictable manner. The general principle is that overload should be managed and controlled such that assets behave in a predictable and coherent manner when under excessive load (as opposed to crashing or exhibiting other unpredictable or undesirable behaviours). Overload control techniques include load balancing, rate limiting, packet dropping, timeout adjustment, queueing, prioritization and other techniques.

Overload controls should be implemented at the UE to detect and mitigate against DoS attacks or an unexpected increase in data traffic from the 5G network. The UE should be configured to have rate limiting controls, and to send alerts to the monitoring systems when its resources have exceeded a pre-defined threshold. CIIOs should monitor the system logs for possible DoS or other attack attempts if there are frequent overload warnings.

Scenarios where the 5G network is overloaded should be included in the CIIOs' business continuity plans, to ensure that the CIIO will still provide its essential services in such events. CIIOs could also plan for sufficient buffers in their networks to be more resilient against unexpected overloads.

4.13 Resilience Against Downgrade Attack

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Downgrade attacks aims to force systems to use protocols with lower levels of security. Threat actors could attempt to force a UE to use lower security levels where there are security vulnerabilities at the communications negotiation process.

There should be controls put in place within the UE to only permit connections to the intended mobile network or 5G network slice. While 5G networks are designed to be more secure, attackers could attempt bidding down[3] attack, such as forcing the UE connection down to 3G/4G[4] or WiFi, to carry out further attacks. While connectivity to other types of networks could be deployed for resilience, system operators should be alerted when the connection of UE have changed. CIIOs should also understand the cybersecurity risks involved in using other communication technologies such as SMS[5], WiFi[6], Bluetooth[7], and other device-to-device communications. The UE could also be configured such that system administrator privileges are required to connect to alternate networks.

In addition to forcing UE to connect to less secure networks, attackers could also force UE to use protocols with weaker protection (e.g., downgrade from HTTPS to HTTP). The system should be configured to use the intended protocols only and system operators should be alerted when there are any deviations from the norm.

4.14 Monitoring of Devices Over the 5G Network

Lifecycle Stages	
Development & Implementation	Operations & Maintenance

Monitoring of devices refers to continuous checking, supervising or determination of the status of devices to identify changes.

UEs should be centrally monitored so system operators would be informed of any abnormalities and security incidents. As 5G network coverage spans a large area, system operators should also monitor the physical location of the UE to detect if there has been unauthorised relocation of the devices. For systems where the UE are designed not to have constant connection to the 5G network, such as for IoT sensors that need to conserve their battery power, system operators should be alerted when UE fail to connect to the monitoring system after its predefined interval. These devices could also be configured to connect to the 5G network and alert the system operators in the event of any unauthorised access or tampering.

[3] Bidding down attack is a cryptographic attack causing devices to downgrade to lower-quality network protocols causing a degradation in cybersecurity posture and quality of service.
[4] Network protocols such as Signaling System 7 (SS7) is a backend signaling protocols widely used for 3G networks which have known vulnerabilities; Diameter signal protocol used by 4G could face similar threats as SS7 because of possible cross-protocol attacks.
[5] An adversary could exploit signalling system vulnerabilities to redirect SMS messages (e.g., 2FA SMS messages).
[6] Insecure Wi-Fi networks could allow adversaries to eavesdrop on connections, leading to possible loss of confidentiality.
[7] Adversary could exploit the lack of strong authentication during the Bluetooth pairing process to compromise mobile device (e.g., Bluesnarfing) as well as to compromise of information transmitted.

Mapping of Recommendations to the 5G Threats

The corresponding recommendations that may help to mitigate each of the 5G threats based on the STRIDE model are mapped in the table below. CIIOs could apply the recommendations in their environment based on the priority of their threats. For systems which have not been deployed, the recommendations that are labelled to be applied at the Development & Implementation stages should be considered at the systems' project initiation.

5G Threats	Impact			Recommendation
	C	I	A	
Spoofing (S)	🟨	🟨	🟨	• 4.1 – Assurance of User Equipment • 4.2 – Segregation of Traffic • 4.3 – Data Protection • 4.4 – System Hardening • 4.5 – Physical Security • 4.7 – Awareness of 5G Threat • 4.8 – Support Requirements from 5G Service Providers • 4.9 – Configuration Management • 4.10 – Access Control • 4.11 – Asset Management • 4.13 – Resilience Against Downgrade Attack • 4.14 – Monitoring of Device over the 5G Network
Tampering (T)		🟨		• 4.1 – Assurance of User Equipment • 4.2 – Segregation of Traffic • 4.3 – Data Protection • 4.4 – System Hardening • 4.5 – Physical Security • 4.7 – Awareness of 5G Threat • 4.9 – Configuration Management • 4.10 – Access Control • 4.13 – Resilience Against Downgrade Attack • 4.14 – Monitoring of Device over the 5G Network
Repudiation (R)		🟨		• 4.1 – Assurance of User Equipment • 4.2 – Segregation of Traffic • 4.3 – Data Protection • 4.4 – System Hardening • 4.5 – Physical Security • 4.9 – Configuration Management • 4.10 – Access Control • 4.13 – Resilience Against Downgrade Attack • 4.14 – Monitoring of Device over the 5G Network
Information Disclosure (I)	🟨			• 4.1 – Assurance of User Equipment • 4.2 – Segregation of Traffic • 4.3 – Data Protection • 4.4 – System Hardening

	🟨			• 4.5 – Physical Security • 4.7 – Awareness of 5G Threat • 4.8 – Support Requirements from 5G Service Providers • 4.9 – Configuration Management • 4.10 – Access Control • 4.13 – Resilience Against Downgrade Attack • 4.14 – Monitoring of Device over the 5G Network
Denial of Service (D)			🟨	• 4.2 – Segregation of Traffic • 4.4 – System Hardening • 4.6 – Business Continuity Planning • 4.7 – Awareness of 5G Threat • 4.10 – Access Control • 4.12 – Overload Controls • 4.13 – Resilience Against Downgrade Attack • 4.14 – Monitoring of Device over the 5G Network
Elevation of Privilege (E)	🟨	🟨	🟨	• 4.1 – Assurance of User Equipment • 4.2 – Segregation of Traffic • 4.4 – System Hardening • 4.5 – Physical Security • 4.7 – Awareness of 5G Threat • 4.8 – Support Requirements from 5G Service Providers • 4.9 – Configuration Management • 4.10 – Access Control • 4.14 – Monitoring of Device over the 5G Network

Table 3 – Mapping of 5G Threats with Recommendations

5. Case Studies

This section showcases two examples to demonstrate how our recommendations can be applied for different use cases. The examples involve systems that belong to CIIOs that may or may not be CII systems providing essential services.

Security should be considered at all stages of the lifecycle from initial development and implementation till operations and maintenance. The advantage of introducing security considerations throughout is to make security threats more visible and widely understood by senior management and other stakeholders.

5.1 Maritime Sector Case Study

Automated Guided Vehicle System

Ports are always finding ways to maximise goods flow and shorten time taken to receive, unload and load containers as part of their business requirements. With ultra-low latency and high reliability of 5G systems, mobile port equipment can be integrated more seamlessly to handle cargo faster and safer in the logistics chain.

Figure 6: Automated Guided Vehicle in action (Source: Business Times Singapore)

Threat Scenario: A disgruntled employee used his team leader’s system credentials to gain unauthorised remote access over the 5G network to one of the Automated Guided Vehicle (AGV) to modify its decision-making parameters, causing disruptions in the port’s operations. Thereafter, the employee hid traces of the modifications by deleting the log files in the AGV. The compromised AGVs made consistent navigational errors, resulting in operational inefficiencies within the ports, which were challenging to troubleshoot due to the logs being removed.

THREATS

Spoofing (S)

Tampering (T)

Repudiation (R)

Information Disclosure (I)

Denial of Service (D)

Elevation of Privilege (E)

Threats identified from the scenario using the STRIDE model are: Tampering, Repudiation and Denial of Service.

Impact: Data integrity of the system and availability of the service are compromised. Furthermore, there could be physical damage to the port and safety risks to the people working in the port.

Based on the threats of Tampering, Repudiation and Denial of Service, the list of recommendations which can mitigate the risks of the threat scenario are:

- Assurance of User Equipment
- Segregation of Traffic
- Data Protection
- System Hardening
- Physical Security
- Business Continuity Planning
- Awareness of 5G Threat
- Configuration Management
- Access Control
- Overload Controls
- Resilience Against Downgrade Attack
- Monitoring of Device over the 5G Network

Improvements to the Access Control policy is the key recommendation for the above threat scenario. Access controls policies could require administrators to log in using multiple authentication factors to make changes to critical system configuration. The policies could also require administrators to make critical changes on site, where there would be physical security measures in place to deter potential threat actors.

In addition, the Configuration Management process could have required the project deployment team to store the last good deployment configuration of the AGVs in a centralised location, which could be used to quickly rectify the unauthorised changes made by the disgruntled employee. Centralised backup of logs could also mitigate against attempts by threat actors to modify or delete records.

5.2 Healthcare Sector Case Study

Healthcare IoT system

Hospitals leverage technology to monitor patients' health accurately and efficiently. With the massive connectivity and low latency offered by 5G networks, large number of IoT devices can be deployed across a hospital to maintain constant monitoring of patients' health conditions and allow faster diagnoses to the patients in need.

Figure 7: IoT Medical Device (Source: IEEE)

Threat Scenario: Some of the medical IoT sensors have been recently replaced by the maintenance vendor and the factory default administrator profiles were not removed as they felt that the sensors were not visible to the public.

An adversary visited the hospital and exploited a known 5G vulnerability to scan for devices connected through 5G in the vicinity and discovered the medical IoT sensors. He managed to use the factory default credentials of the new sensors to gain access to the patient data stored in them. Next, he performed privilege escalation to obtain root access to the sensors, allowing him to modify data transmitted by the devices, causing wrong diagnoses. The adversary then used the compromised sensors to carry out DoS attacks on the hospital's internal servers as they were trusted by the network. The hospital could not receive real-time information of the patients throughout the period of the DoS attack and the healthcare workers were not able to attend to the patients timely.

THREATS

Spoofing (S)

Tampering (T)

Repudiation (R)

Information Disclosure (I)

Denial of Service (D)

Elevation of Privilege (E)

Threats identified from the scenario using the STRIDE model are: Tampering, Information Disclosure, Denial of Service and Elevation of Privilege

Impact: Loss of availability of the hospitals IoT system due to DoS to its internal servers and loss of control to its IoT devices, which would adversely impact operational capabilities of the hospital. Tampering of data stored and transmitted causes a loss of data integrity, which could compromise the safety of patients. There is also data confidentiality concern as sensitive patient data may be exfiltrated from the system.

Based on the threats of Denial of Service, Elevation of Privilege, Tampering and Information Disclosure, the list of recommendations which can mitigate the risks of the threat scenario are:

- Assurance of User Equipment
- Segregation of Traffic
- Data Protection
- System Hardening
- Physical Security
- Business Continuity Planning
- Awareness of 5G Threat
- Support Requirements from 5G Service Providers
- Configuration Management
- Access Control
- Overload Controls
- Resilience Against Downgrade Attack
- Monitoring of Device over the 5G Network

System Hardening and Overload Controls are the most effective measures to prevent the above threat scenario from occurring. Robust system hardening processes will require the hospital's IT project team to ensure that default credentials are not used after they have been deployed. Overload controls can also be implemented on the server to allow it to inform system operators once performance thresholds have been reached or ignore overwhelming request from the IoT sensors.

Other mitigating measures such as Awareness of 5G Threats and Business Continuity Planning could have allowed the IT and Security teams within the hospital to take pre-emptive actions to mitigate the 5G vulnerability which the adversary used to scan and connect to the IoT medical devices, and to prepare for scenarios where they lose control to some of their IoT medical devices.

6. Terms and Definitions

Terms	Definitions
Access Control	Access functions, which include identification, authentication, authorisation, and accountability
Authentication	Act of confirming the identity of an entity
Authorisation	Act of specifying the access permissions to a resource
Availability	Ensuring timely and reliable access to and use of information
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes
Denial of service (DoS)	Prevention of authorised access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorised users
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity
Internet of Things (IoT)	System of physical and virtual entities that are connected with one another allowing interaction anytime, anywhere
Multi-access Edge Computing (MEC)	The 5G software defined network introduces multi-access edge computing (MEC) which pushes virtualised computing activities outward to the edge of the 5G network (i.e., nearer to the base stations)
Mobile Network Operators (MNO)	Entities providing mobile network services to users, operating their own network or with the help of third parties
User Equipment (UE)	A subscriber’s device, such as a cell phones, tablets, modems, or any other equipment capable of connecting to 5G services

7. Abbreviations and Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
5G	5th Generation
5G NR	5G New Radio
5G RAN	5G Radio Access Network
CIA	Confidentiality, Integrity, Availability
CII	Critical Information Infrastructure
CIIO	Critical Information Infrastructure Owner
CLS	Cybersecurity Labelling Scheme
CSA	Cyber Security Agency of Singapore
DDoS	Distributed Denial of Service (attack)
DoS	Denial of Service (attack)
EECC	European Electronic Communications Code
eMBB	enhanced Mobile Broadband
eNB	Evolved Node B
ENISA	European Union Agency for Network and information Security
gNB	Next Generation Node B
GSMA	Global System for Mobile Communications Association
HTTP	Hypertext Transfer Protocol
IMDA	Info-communications Media Development Authority
IMEI	International Mobile Equipment Identity
IoT	Internet of things
IT	Information Technology
MITM	Man-In-The Middle
mMTC	massive Machine-Type Communication
MNO	Mobile Network Operator
NSA	Non-Standalone
QOS	Quality of Service
SA	Standalone
SDLC	System Development Lifecycle
SIM	Subscriber Identity Module
SLA	Service Level Agreement
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege
TPM	Trusted Platform Module
UE	User Equipment
URLLC	Ultra-Reliable Low-Latency Communication

8. Reference

S/N	Document	Source	Dated
1	Security Guidance for 5G cloud infrastructures Part I: Prevent and Detect Lateral Movement	CISA	Oct 2021
2	Security Guidance for 5G cloud infrastructures Part III: Data Protection	CISA	Dec 2021
3	Potential threat vectors to 5G infrastructure	CISA	May 2021
4	Guide to Cyber Threat Modelling	CSA	Feb 2021
5	Guide to conducting Cybersecurity Risk Assessment for Critical Information Infrastructure	CSA	Feb 2021
6	Guideline for Auditing Critical Information Infrastructure	CSA	Jan 2020
7	Security by Design Framework	CSA	Nov 2017
8	Threat Landscape for 5G Network	ENISA	Dec 2020
9	Security in 5G Specifications	ENISA	Feb 2021
10	5G Supplement	ENISA	Jul 2021
11	Guideline on Security Measures under the EECC	ENISA	Jul 2021
12	5G Implementation Guideline	GSMA	Jul 2019
13	Guidelines Internet of Things (IoT) Cyber Security Guide	IMDA	Mar 2020
14	Microsoft Threat Modelling Tool	Microsoft	Apr 2018
15	Security Considerations for 5G Network Operation	NGMN	Aug 2021
16	NIST SP 800-39, Managing Information Security Risk	NIST	Mar 2011
17	NIST SP 800-41, Guidelines on Firewalls and Firewall Policy	NIST	Sep 2009
18	NIST SP 800-12, An Introduction to Computer Security	NIST	Jun 2017
19	NIST Computer Security Resource Centre Glossary	NIST	-

Annex A – 3GPP 5G Security Enhancements

As part of the work of 3GPP specifications, 5G offers enhanced security features with better resilience and protection against security threats compared to 3G/4G. The security features include:

i. The Subscriber Permanent Identifier (SUPI) enhances subscriber privacy to mitigate against the threats from IMSI catchers. SUPI is encrypted when sent over-the-air as a one-time temporary identifier called the Subscriber Concealed Identifier (SUCI).

ii. Additional higher protocol layer security mechanisms to protect the new service-based interfaces - 3GPP specifies new security requirements that are designed to ensure that network functions are securely exposed. 3GPP have defined requirements for 5G Standalone network functions to support Transport Layer Security (TLS) encryption for the connections between them.

iii. Integrity protection of user data over the air interface will protect the traffic from unauthorised modifications and hence together with encryption, provides full-fledged protection for the user plane over the air. These features at the user plane mitigates against eavesdropping and modification attacks.

iv. Flexible authentication framework in 5G which allows the 5G Core to serve access requests from Wi-Fi and wireline devices as well as from 5G devices which enable different types of authentication methods in addition to SIM cards.

v. New authentication features such as “Home Control” enable MNOs to mitigate fraud and prevent privacy attacks against their subscribers when roaming.

vi. 3GPP specifies mutual authentication between the network slice manager and the slices to achieve network slice security. Network slice policies can also be put in place to assure effective isolation of the physical and logical network slices to ensure threats does not traverse between them.

Annex B – 5G Threats and Recommendations Checklist

S/N	5G Recommendation	Lifecycle Stages		Threat Mapped						Yes / No
4.1	Assurance of User Equipment	D & I	O & M	S	T	R	I	D	E	
4.2	Segregation of Traffic	D & I	O & M	S	T	R	I	D	E	
4.3	Data Protection	D & I	O & M	S	T	R	I	D	E	
4.4	System Hardening	D & I	O & M	S	T	R	I	D	E	
4.5	Physical Security	D & I	O & M	S	T	R	I	D	E	
4.6	Business Continuity Planning	D & I	O & M	S	T	R	I	D	E	
4.7	Awareness of 5G Threat	D & I	O & M	S	T	R	I	D	E	
4.8	Support Requirements from 5G Service Providers	D & I	O & M	S	T	R	I	D	E	
4.9	Configuration Management	D & I	O & M	S	T	R	I	D	E	
4.10	Access Control	D & I	O & M	S	T	R	I	D	E	
4.11	Asset Management	D & I	O & M	S	T	R	I	D	E	
4.12	Overload Controls	D & I	O & M	S	T	R	I	D	E	
4.13	Resilience Against Downgrade Attack	D & I	O & M	S	T	R	I	D	E	
4.14	Monitoring of Devices Over the 5G Network	D & I	O & M	S	T	R	I	D	E	

Lifecycle Stages

D & I : Development & Implementation

O & M : Operations & Maintenance

Threat

S	*: Spoofing*
T	*: Tampering*
R	*: Repudiation*
I	*: Information Disclosure*
D	*: Denial of Service*
E	*: Elevation of Privilege*

QUERIES & FEEDBACK

Questions and feedback on this document may be submitted to:

CSA-TCPO@csa.gov.sg