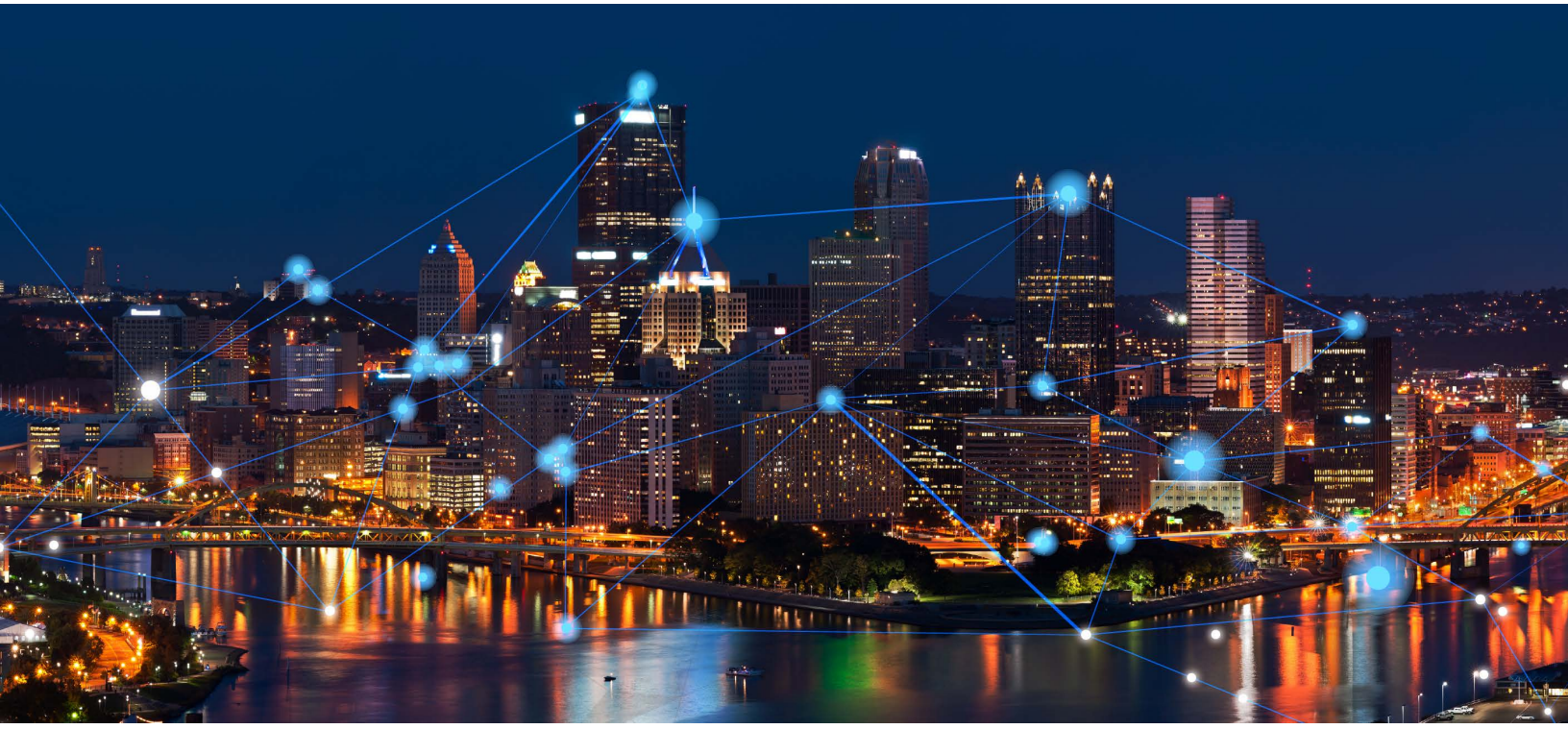

5G Security Evaluation Process Investigation

Version 1

May 2022

ACKNOWLEDGEMENTS

The study group leads from the Cybersecurity and Infrastructure Security Agency (CISA), Vincent Sritapan, the DHS Science and Technology Directorate (S&T), Brent Talbot, and the Department of Defense (DoD), Dr. Dan Massey, thank all who collaborated on this effort, whether by authoring and contributing to the investigation or by reviewing and providing feedback. Collaborators are:

Name	Organization
Vincent Sritapan, CISA Study Group Lead	CISA Cybersecurity Division
Dr. Daniel Massey, DoD Study Group Lead	DoD Under Secretary of Defense for Research and Engineering
Brent Talbot	DHS Science & Technology Directorate
Serena Reynolds	CISA National Risk Management Center
Daniel Dagher	CISA National Risk Management Center
DeLana Hill	CISA
Lilian Herrera	CISA
Ruben Yabut	CISA National Risk Management Center
Steven Slater	CISA
Debra Stanislawski	DoD
Jennifer Peyrot	DoD
Sergio LaPorte	DoD
Scott Brinson	DoD
Dr. Mark Stanley	DoD
Joshua Weaver	DoD
Dr. Aaron Hansen	DoD
Gema Howell	National Institute of Standards and Technology
Jeffrey Cichonski	National Institute of Standards and Technology
Dr. DJ Shyy	The MITRE Corporation
Dr. Mari Spina	The MITRE Corporation
Demetrius Davis	The MITRE Corporation
Doug White	The MITRE Corporation
Terri Phillips	The MITRE Corporation

EXECUTIVE SUMMARY

Standards for Phases 1 and 2 of fifth generation (5G) cellular network technology are complete and cellular operators now are rolling out 5G services. Federal agencies have used mobile wireless for several years; however, prior to 5G, agencies tended to treat the cellular network solely as a pipe for transport layer communications. With 5G, agencies want to take advantage of different 5G usage scenarios: low-, mid-, and high-band spectrum. The new features, capabilities, and services 5G offers can transform mission and business operations.

To move an unclassified federal system from prototype to production, a security assessment is required to receive authorization to operate (ATO). Because the deployment of 5G standalone architecture (SA), multi-access edge computing (MEC), and network slicing are in the early stages, the federal government has an opportunity to examine and understand security challenges that 5G services and features may present for system security ATO before these features are widely deployed by cellular operators. It is important for the government to employ a flexible, adaptive, and repeatable approach to evaluating the security and resiliency of any 5G network deployment. Further, the approach may need to extend beyond assessing the system's compliance with existing federal cybersecurity policies, regulations, and best practices to address known attack vectors, yet-to-be-discovered threats, and implementation-specific vulnerabilities.

This study investigates how 5G may introduce unique challenges to the traditional ATO process defined in security assessment processes and frameworks such as the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF). This study is a joint effort between DHS Science and Technology Directorate (S&T), the Cybersecurity and Infrastructure Security Agency (CISA), and DoD Under Secretary of Defense for Research and Engineering. Each of these agencies is currently active in 5G research and security.

5G System

The 5G technology ecosystem is complex and still evolving. Any 5G cybersecurity assessment approach must continually extend and evolve as new 5G standards, threat vectors, deployment features, and policies are introduced. A common understanding and lexicon is also required to identify and describe critical elements, functions, relationships, and processes.

To determine how inclusion of 5G technologies in a federal system might impact the ATO process, it is necessary to complete the following steps:

- Define a 5G ***system model*** as a common lexicon and reference.
- Understand the differences between 5G and fourth generation (4G) system architecture and security.
- Understand the types of threats that must be evaluated as part of a system-level risk assessment.

5G Security Evaluation Process

The study team developed the proposed five-step 5G Security Evaluation Process shown in Figure ES-1 to conduct its investigation. The process identifies important threat frameworks, 5G system security considerations, industry security specifications, federal security guidance documents, and relevant organizations and methodologies for cyber assessment of 5G systems. It also identifies potential gaps in existing security guidance for some new 5G features and services.

Figure ES-1. Proposed 5G Security Evaluation Process

From its investigation, the study team concluded that, as stated in the ***NIST RMF***, the RMF is technology-neutral and ***does not need to be modified for 5G***. The ***proposed 5G security evaluation process can support*** government agency ***activities during the RMF system-level "Prepare" step for 5G-enabled systems***. The proposed five-step process is intended to be repeatable and can be applied to a wide array of 5G system architectures, deployment scenarios/use cases, and operational environments. Step 1 calls for a use case definition to identify 5G subsystems that are part of the system, component configurations, applications, and interfaces involved in the operation of the system. The complexity of 5G technology makes the process of defining the security assessment boundary for a federal ATO challenging. Consequently, Step 2 involves defining the boundary to identify the technologies and systems requiring assessment and authorization (A&A), taking into consideration the ownership and deployment of the products and services that comprise the use case.

After defining the assessment boundary, Step 3 includes conducting a high-level threat analysis of each 5G subsystem to identify the mitigating cybersecurity capabilities (e.g., identity, credential and access management; network security; and communication and interface security) that need to be addressed by A&A activities.

Step 4 involves creating a catalog of federal security guidance that includes the RMF, NIST's Cybersecurity Framework, supply chain risk management, the Federal Risk and Authorization Management Program (FedRAMP), other NIST and federal cybersecurity guidance relevant to the security capabilities, as well as relevant industry specifications.

Step 5 examines the alignment between security requirements and federal security guidance and assessment programs. Where a security requirement exists but no assessment guidance is available to guide A&A activities, a gap is identified and alternatives to remediating assessment deficiencies can be addressed. For example, if no federal assessment guidance exists for the Open Radio Access Network (O-RAN), an international or commercial program such as the O-RAN Alliance's test and integration center certification may be considered.

This document provides an overview of the proposed 5G Security Evaluation Process and applies the process to an example private 5G network use case to demonstrate considerations for each step within the overarching process.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

The first wave of fifth generation (5G) technology adoption across the public sector is expected to comprise a small set of common use cases and "starter" 5G projects. In many instances, government-furnished mobile devices will access non-standalone (NSA) 5G mobile networks managed by mobile network operators (MNOs) or communication service providers. A broader set of advanced 5G features including security will be available when 5G standalone (SA) networks are deployed at scale; however, to realize these new communications capabilities, core network infrastructure upgrades will be required.

During this period of network infrastructure upgrades, rapidly evolving technical standards, a vibrant global marketplace (comprised of many new entrants to the telecommunications market), and a fluid and diverse threat landscape, it is important for the government to employ a flexible, adaptive, and repeatable approach to evaluating the security and resiliency of any 5G network deployment. Such an approach must extend beyond assessing the system's compliance with standing government cybersecurity policies, regulations, and best practices to address known attack vectors, yet-to-be-discovered threats, and implementation-specific vulnerabilities.

This document proposes a five-step 5G security evaluation process that can be applied to a wide array of 5G system architectures, deployment scenarios, and operational environments. The comprehensive process includes cataloging and mapping applicable threats and vulnerabilities as well as mitigating attributes and security capabilities.

1.1 Motivation

5G networks are designed to be more secure than 4G. However, the complexity of 5G networks—with new features, services, and an anticipated massive increase in the number and types of devices they will serve, coupled with the use of virtualization and disaggregation of the Radio Access Network (RAN) and the 5G Core—expands the threat surface and can make defining the system boundary challenging. Federal enterprises implementing—or planning to implement—5G-enabled systems may not be aware of how inclusion of 5G technologies impacts the system risk assessment/authorization to operate (ATO) process. Further, with the deployment of 5G being in its early stages, Federal enterprises may not have ready access to or awareness of the potential threats and security capabilities that 5G offers.

A full-scope security evaluation of a highly virtualized, distributed, multi-vendor ecosystem can easily involve several evaluation and approval steps, communications across multiple stakeholders, and varying levels of compliance guidance and regulations. A tedious, costly, and time-consuming security evaluation process would likely impede 5G adoption across the public sector and may lead some organizations to accept greater levels of risk to conserve resources.

The level of effort and resources required by enterprise stakeholders and mission owners to fully assess a 5G network and accompanying system elements varies based upon several factors such as the total number of unique equipment and disaggregated network functions. However, the repeated acquisition and use of common 5G network components will minimize the steps and time to conduct an end-to-end 5G system security assessment. This document presents examples of common 5G subsystems and components to highlight the efficiencies gained during each of the five steps of the proposed 5G Security Evaluation Process.

This document also presents a set of potential 5G "starter" projects beyond the commercial mobile broadband offerings currently offered by national and regional MNOs for federal agencies.

1.2 Purpose

5G exploration, experimentation, and prototyping are underway at multiple federal agencies [1]. For federal agencies to move a system from prototype to production, a security assessment is required to receive ATO for Federal Information Security Modernization Act compliance. The complexity of 5G technology makes the process of defining the security authorization boundary challenging. With deployment of 5G SA in early stages, the federal government has an opportunity to examine and understand security challenges that 5G services and features may present for system security assessment and authorization (A&A).

This paper presents the results of an investigation into how inclusion of 5G technologies in an unclassified federal system may introduce unique challenges to the traditional ATO process defined in security assessment processes and frameworks such as the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) [2], the Cyber Security Framework (CSF) [3], and the Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) framework [4] for its contractors.

This study is a joint effort between the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), DHS Cybersecurity and Infrastructure Security Agency (CISA), and the DoD Under Secretary of Defense for Research and Engineering. Each of these agencies is currently active in 5G research and security.

To guide its investigation, the DHS/DoD study team developed the proposed 5G Security Evaluation Process described in this document. The team concluded that the proposed process does not replace existing assessment frameworks. Instead, it is intended to be a repeatable methodology that federal program/project managers can use as they conduct the ***Prepare*** step of the NIST RMF for a 5G-enabled system. The threat analysis, identification of mitigating security capabilities, alignment to federal security guidance, and discovery of potential gaps in existing federal guidance is provided as a resource to help federal enterprises assess risks relevant to their 5G-enabled system, determine security requirements, and identify areas needing additional attention. The document's intended audience is federal 5G program and project managers and executives responsible for designing, deploying, and securing federal systems that use 5G technologies.

1.3 Document Structure

This document provides an overview of the 5G Security Evaluation Process with an example use case demonstrating considerations for each step. To provide context for the process, it includes a brief overview of 5G security, the system model used as reference, and a summary of the types of threats that may impact 5G subsystems.

- Section 2 describes the 5G system model used as a reference for the process, explains some of the differences between 4G and 5G, highlights some 5G security improvements, and discusses high-level threats to 5G subsystems.
- Section 3 describes the proposed 5G security evaluation process and applies the process to a notional private 5G network deployment scenario.

- Section 4 summarizes the document's conclusions.
- Appendix A contains the list of 5G Reference Designs defined in the 5G system model.
- Appendix B discuses risks of 5G deployments from a program manager's perspective.
- Appendix C presents a description of security categories for Step 3 of the process.
- Appendix D provides additional information on 5G network slice security.

2 5G OVERVIEW

The 5G technology ecosystem is complex and still evolving. Any 5G cybersecurity assessment approach must extend and evolve as new 5G standards, threat vectors, deployment features, and policies are introduced. Moreover, a common understanding and lexicon is needed to identify and describe critical elements, functions, relationships, and processes. To investigate the need for a 5G security evaluation process, it is necessary to:

- Identify a 5G system model to serve as the lexicon for 5G and delineate the 5G attack surface for the investigation.
- Describe 5G and how it differs from prior generations of cellular technology.
- Understand—at a high level—the types of threats that could impact a 5G-enabled system.

2.1 5G System Model

A 5G system includes User Equipment (UE), 5G RAN, and 5G Core, and may include Multi-Access Edge Computing (MEC) and/or Network Slicing. Because of the extensive use of virtualization in 5G and the critical need for secure network orchestration and management, these subsystems also are included in the *5G* system model shown in Figure 1 below. Each top-level 5G system component may be represented as a single subsystem configuration or a collection of component configurations. 5G networks likely will include multiple service providers (e.g., cloud, communications, or application service providers for MEC or Core), thereby introducing additional complexity to the security risk assessment. Recognizing this facet of 5G, Figure 1 shows that each 5G subsystem has a set of attributes (e.g., whether the 5G system uses SA or NSA architecture or whether UE can be updated/patched, authenticated, or centrally managed, or who owns the RAN and whether it is virtualized). This 5G system decomposition enables unique functions and system attributes to be applied to system components, serves as the reference model for the 5G security evaluation process investigation, and facilitates the identification of 5G threats.

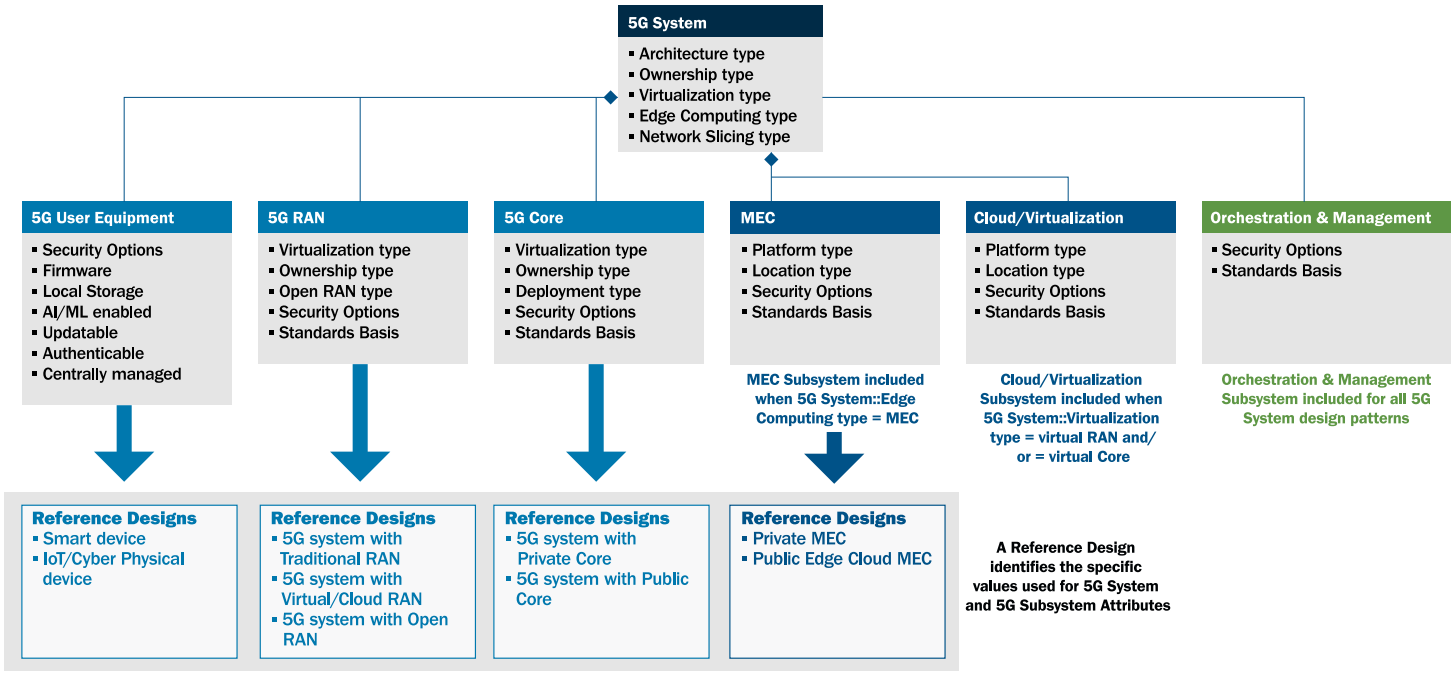

Figure 1. 5G System Model

The middle tier depicted in Figure 1 presents the following 5G subsystems:

- **5G UE** allows a user access to network services. A wide range of possible device types are supported with 5G (e.g., internet of things [IoT], autonomous vehicles). The components of 5G UE include hardware, software, a subscriber identity module (SIM) and interfaces (air interface, local ports, and sensors).
- **5G RAN** supports all the logical access functions to connect UEs to the 5G system via the 5G New Radio (NR) air interface. While the 5G Core network supports interworking with other types of Access Networks, only the 5G RAN is included in the scope of the 5G Security Evaluation process investigation. The 5G RAN includes a central unit, distributed unit, radio unit, multiple interfaces (e.g., air interface, midhaul, backhaul, management), and may also include a RAN Intelligent Controller to control Open Radio Access Network (O-RAN) configuration and optimization.
- **5G Core** authenticates subscribers, establishes reliable, secure connectivity to the network for end users, and provides access to its services. In addition to a set of interfaces (UE, RAN, intra-core, etc.), the 5G Core includes a set of functions for the control plane, user (data) plane, network data (for other Core functions), application functions that enable external applications to connect to Core functions, and network slicing.
- **MEC** is a cloud service running at the edge of the network providing specific tasks in real time or near real time. MEC moves computing power closer to the end user to enable applications and services requiring unique connectivity characteristics such as ultra-low latency. In addition to MEC interfaces, the MEC includes a system-level component and a host-level component, both of which further decomposes to the MEC host (platform and virtualization infrastructure) and MEC host management.

- **Cloud/Virtualization** is necessary when a virtualized or cloud deployment model is used. and represents the underlying infrastructure support for those virtual functions. It could be set up as a single virtualized platform or multiple interconnected virtual platforms (i.e., cloud). This subsystem comprises infrastructure, a virtualization layer that abstracts hardware resources from the infrastructure, resource orchestration functions for the subsystem components, a set of interfaces, and network functions that are deployed as virtual (virtual network function [VNF]) or cloud-native container (cloud-native network function [CNF]) components.
- **Orchestration and Management** includes all network management functions (Fault, Configuration, Accounting, Performance, Security) as well as any orchestrator functions supporting deployment and management of virtualized infrastructure for the 5G RAN, 5G Core, MEC, and Cloud/Virtualization subsystems.

The lowest tier within Figure 1 depicts ***reference designs***, which represent a common implementation of a 5G subsystem, (i.e., when traditional RAN, virtual RAN, and O-RAN are reference designs for the RAN subsystem). In addition to the attack surface for each 5G subsystem, a reference design may introduce additional threats such as additional interfaces for O-RAN that do not exist in traditional RAN. This level of abstraction should facilitate risk assessments by multiple domain subject matter experts and engagement by non-technical stakeholders and decisionmakers. A few example 5G reference designs are presented in Figure 2.

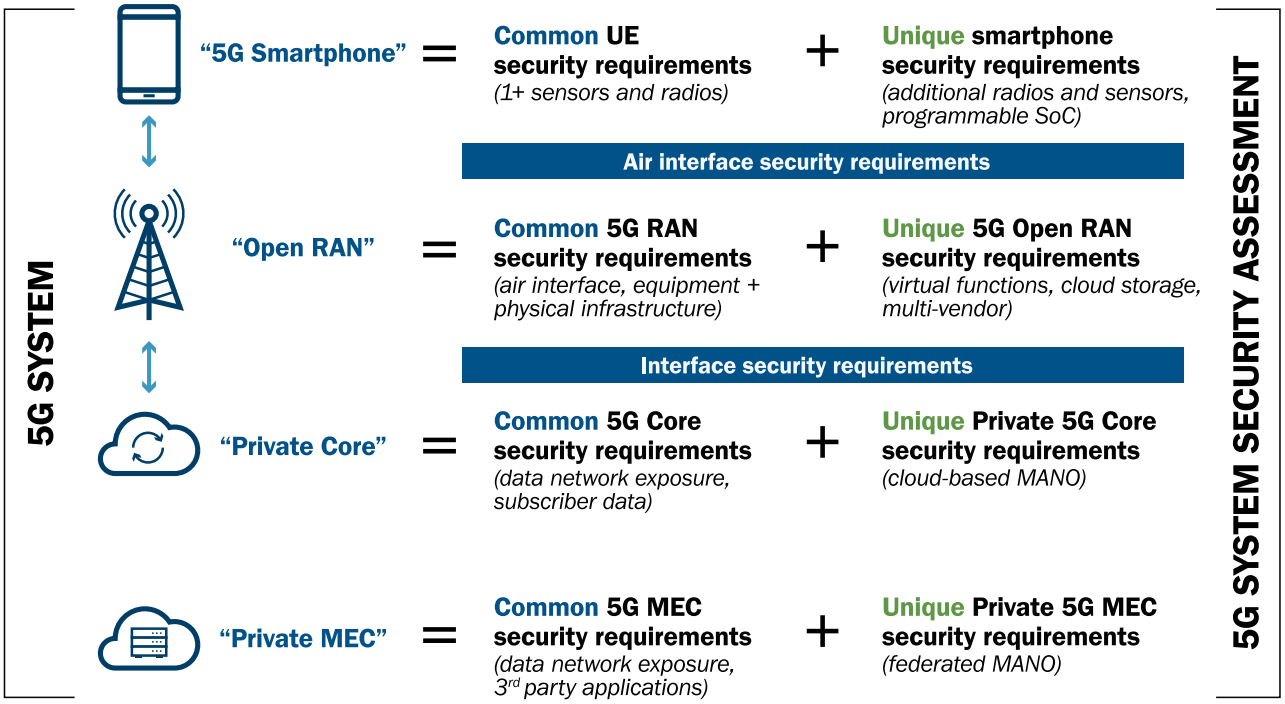

Figure 2. Top-Level 5G System Reference Design

The four example reference designs in Figure 2 may be combined to represent a single 5G system. One representation each for a 5G UE, RAN, Core, and MEC solution shows how security requirements for a "generic" subsystem (e.g., generic UE) can be extended to include additional security requirements introduced by the internal "unique" solution architecture (e.g., hardware, software, and interfaces), as well as functions and attributes defined for the given reference design

(e.g., additional sensors, radios, and computing capacity for a smart device). These requirements are critical inputs to the proposed 5G security evaluation process. As an added benefit, these reference designs may be reused and modified as needed to encapsulate unique functional and operational details of a future 5G system application or use case. (Refer to Appendix A for additional information on reference designs.)

2.2 5G Security

Compared to 4G cellular network technology, 5G will serve more devices of varying types and more use cases. 5G introduces new features and services, including the following:

- NR with enhanced capabilities, increased spectrum, spectrum sharing, and low-, mid-, and high-band frequencies.
- Cell densification to serve large numbers of users and new techniques such as beamforming to direct the wireless communication channel at users and reduce interference.
- MEC, which moves typically centralized applications closer to the edge of the network to reduce latency, sustain high data transfer rates, and ingest high volumes of data.
- Network slicing to create multiple virtual networks that provide different quality of service levels over shared physical infrastructure.
- Virtualization of the RAN and the 5G Core to dynamically scale network functions.

The Third Generation Partnership Project (3GPP), the main standards-development organization for 5G, has built many security improvements into 5G, highlights of which are summarized in the following table.

Table 1. 5G Security Improvements (Standalone Architecture)

Subscriber Security and Privacy	**RAN Security and Privacy**
• Encryption of unique device identifiers to mitigate rogue base stations. • Mutual authentication of subscriber and network. • Confidentiality and integrity protection for control (signaling) traffic and user (data) traffic. • Ability to restrict radio technologies that a device uses (e.g., turn off 2G/3G).	• Use of a massive number of antennas and beamforming techniques to reduce interference and make it harder to conduct over-the-air eavesdropping attacks. • RAN separated into distributed units (DUs) and centralized units (CUs), with DUs located near the antenna and CUs, which store sensitive information, placed inside a trusted and physically secure location.
Core Network Security	**Roaming Security**
• Shift to service-based architecture with Transport Layer Security-based authentication and encryption. • Options for Internet Protocol Security and attribute-based security across each interface. • Service-based discovery and registration to support confidentiality, integrity, and replay protection.	• Security gateway for roaming interconnects to enforce control plane security policies. • Home network can verify if a device is present in the serving network when it receives a service request from the serving network. • Protection of user plane traffic between two networks.

Network Slicing and Virtualization	Authentication
• Network slicing allows isolation of data plane traffic as well as different security attributes for various user classes. • Software-defined, virtualized network functions allow for rapid reconfiguration to respond to attacks.	• Subscriber authentication is completed by home network (helps protect against false base station attacks). • Authentication is open and agnostic to the RAN. Both 3GPP and non-3GPP access networks (e.g., Wi-Fi) use the same authentication procedures.

2.3 5G Threat Landscape

A key input to any security risk assessment is threat analysis. The 5G system model supports depiction of the attack surface for the investigation. There are numerous threat frameworks such as those offered by MITRE ATT&CK® [5]; the European Union Agency for Cybersecurity's (ENISA) 5G Threat Landscape [6]; the Threat Modeling Framework for Mobile Communication Systems [7]; 3GPP's Security Assurance Specifications (SCAS) and Technical Specification (TS) 33.501 [8]; publications released by the Federal Communications Commission (FCC) Communications Security, Reliability, and Interoperability Council VII (CSRIC) [9]; 5G Enablers for Network and System Security and Resilience (ENSURE) [10]; and the GSM Association's (GSMA) Security Manual [11]. The study team examined these resources as well as threat analyses conducted by 3GPP and a paper on potential 5G threat vectors published by the Enduring Security Framework's 5G Threat Model Working Panel [12]. Figure 3 shows some of the threats to the 5G subsystems that were extracted from these sources. Some of the threats such as eavesdropping, theft of user data, or user location tracking may impact integrity and confidentiality of user data as well as service availability to individual users. Other threats may impact local or regional network, application, or service availability (e.g., denial of service [DoS] or Distributed DoS [DDoS] attacks, misconfigured or compromised virtualization platforms or network functions, vulnerable components [supply chain threats], or physical attacks on edge computing components), with follow-on effects on the confidentiality, integrity, and availability of 5G services and applications for enterprises relying on 5G for their missions.

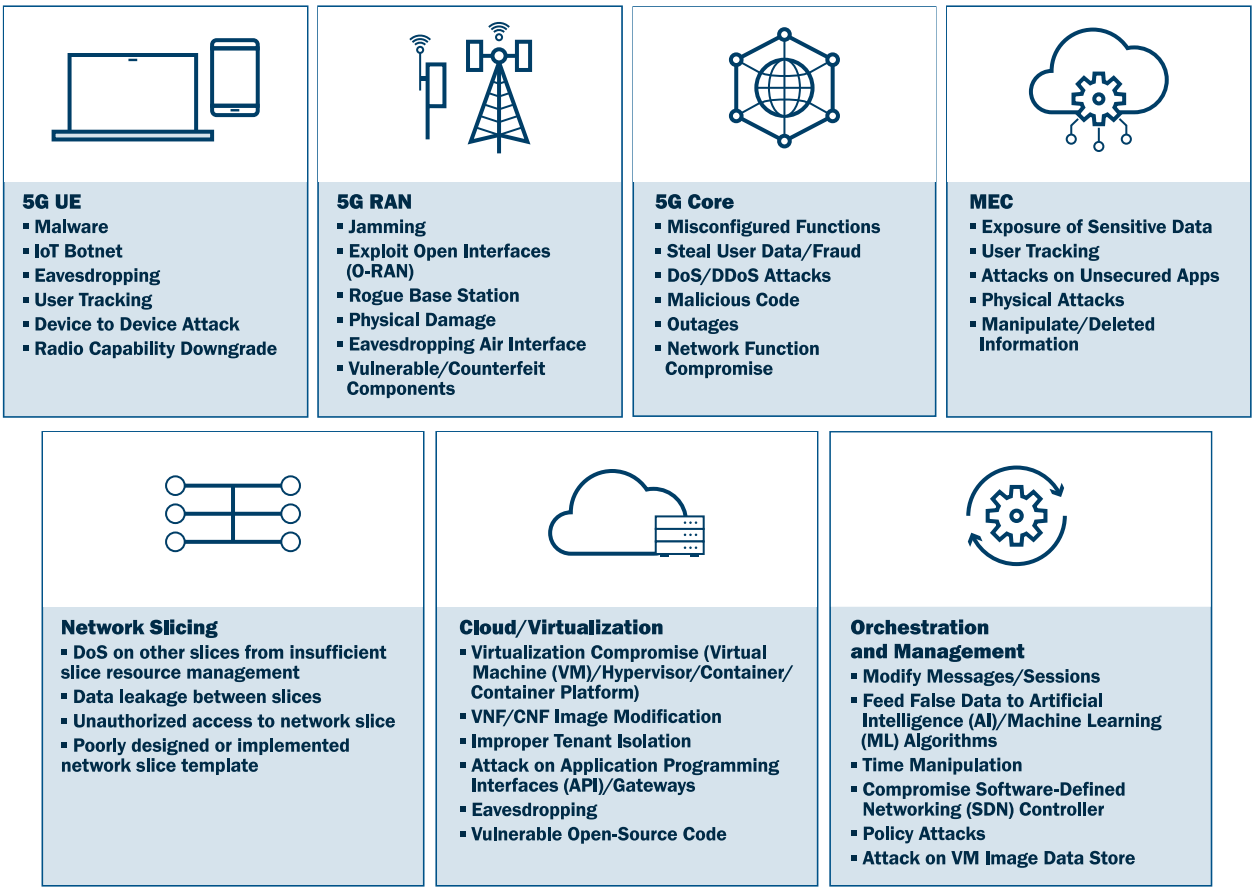

Figure 3. Threats to 5G Subsystems

To aid in describing the threats and as a starting point for agencies developing their own 5G threat models, the study team grouped potential threats into the categories described below. Understanding these threats helps enterprise risk managers prioritize security activities and identify the security capabilities needed to mitigate threats relevant to the 5G systems and subsystems within their 5G-enabled system boundary. The threat categories are:

- **General Cybersecurity Threats:** These threats affect ***all 5G subsystems***, and include misconfigurations, human error, failure to properly harden software and hardware, adversary lateral movement, information spillage, and general unauthorized access attacks. Misconfiguration of components or failure to properly harden hardware or software could be exploited by attackers to reconfigure 5G elements, steer traffic to an attacker, or steal data.
- **Virtualization Threats:** Threats to virtual machine (VM) and container service platforms impact the ***5G Core, RAN, MEC, Network Slicing, Virtualization, and Orchestration and Management***. Threats include DoS, VM/container escape, side-channel attacks, and cloud service consumer misconfigurations. Extreme resource consumption by one tenant in a multi-tenant virtualization environment can create a DoS event for adjacent tenant systems. Such an event can prevent or seriously degrade mission functionality. Similarly, colocation attacks such as VM/container escape or side-channel attacks can put neighboring compute workloads at risk for resource deprivation, lateral movement, and compromise of data confidentiality, integrity, or availability. A side-channel attack on 5G RAN or Core functions can result in the

bypassing of user account permissions, virtualization boundaries, or protected memory regions, leading to the exposure of sensitive information.

- **Network and Management Interface Threats:** These threats impact network, management, and over-the-air interfaces of ***all 5G subsystems*** and include DoS, jamming, eavesdropping, address spoofing, traffic/message tampering, system/protocol discovery, improper tenant traffic isolation, and access control attacks. Over-the-air interface threats are located between the UE and the RAN, where use of radio jamming techniques can cause interference that could prevent access by the UE or cause loss of 5G service. Core network functions that are virtualized/containerized are deployed as tenants on shared cloud infrastructure, where improper isolation of traffic between tenants can expose those virtual environments to unauthorized access or loss of information confidentiality (e.g., subscriber data, network configurations, etc.).
- **Application and Service Threats:** Threats associated with the delivery of 5G applications and services impact ***all 5G subsystems*** and include malware and malicious code injection, DoS and DDoS, Application Programming Interface (API) manipulation, exploitation of software vulnerabilities, and access control attacks. UEs such as smartphones are vulnerable to exploitation of applications and malicious code that can expose private data to threat actors. Unprotected or vulnerable APIs at the MEC could lead to unauthorized access to application and information at the MEC and facilitate further attacks from within the network.
- **Rogue Elements:** Threats from rogue ***UE***, rogue base stations, or Radio Units in the ***RAN*** and rogue network hosts or spoofed components in the ***MEC*** can be used to attack the 5G system. Rogue base stations, for example, can use jamming to force UE to use the rogue base station and then capture user information and location, while rogue or malicious components in the MEC can compromise MEC applications to delete, alter, or steal data.
- **Privacy Threats:** Threats to ***UE*** as well as systems in the ***RAN*** and ***5G Core*** involved in the handling, sharing, storage, and communication of user and user-associated information in a 5G network include eavesdropping, user and device identifier and location tracking, and user, protocol, and system spoofing attacks. An attacker could monitor the air interface between the RAN and UE device to extract an unprotected unique device identifier and track the device user, while unauthorized access to subscriber data stored in the 5G Core could be used for identity theft or telecom fraud.
- **Environmental and Physical Threats:** Vulnerabilities and weaknesses in environmental and physical access control systems, natural disasters, and power outages impact the ***RAN, 5G Core, MEC, and Virtualization*** subsystems. Physical access to ports, equipment, and devices; natural disasters; electromagnetic pulse; and loss of power are predominant concerns. In the RAN, small cells positioned on lamp posts could be subjected to physical theft or damage, while a power outage or natural disaster could damage/render inaccessible RAN nodes or parts of the 5G Core.
- **Supply Chain Threats:** Threats can occur during provisioning, acquisition, and incorporation of software, firmware, and hardware components into ***UE, RAN, 5G Core, and Virtualization*** subsystems. Threats include vulnerable or malicious component insertion, vulnerable or malicious open-source components, and attacks on vulnerable hardware, firmware, or operating systems. Malicious code injection into common code repositories used to build system software for release to production can have grave impacts on operations, especially if

the impacted systems have access to privileged user systems such as those employed for identity and access management or network health and configuration management. Inclusion of firmware/hardware components of unknown provenance or security posture (e.g., in UE or the RAN) can introduce malicious or counterfeit components into these subsystems, creating the potential for exposure of sensitive user and network data to adversaries.

- **Artificial Intelligence/Machine Language (AI/ML) Threats:** Threats to data integrity, confidentiality, and availability of ***UE*** (e.g., gateways for IoT or cyber-physical devices), the ***RAN***, and the ***Orchestration and Management*** subsystems. These threats impact AI/ML software and systems as well as the network elements and services that rely on the accuracy, timeliness, and trustworthiness of the data for decisions based on AI/ML such as dynamic allocation of network functions. For example, corruption in the analytic function code used to execute algorithms or insertion of false or tainted data to the AI/ML algorithms can degrade network operation with potential impact to human safety (e.g., in the use of autonomous vehicles or smart city traffic management).

The 5G security evaluation process investigation focuses on the 5G SA architecture with a 5G Core. However, MNOs will transition to SA over time. During that transition time, which may take years for nationwide deployment, MNOs will use the NSA architecture, which relies on a 4G (Long-Term Evolution) Core, thus inheriting known 4G vulnerabilities [9].

This threat information can be used by system security officials and project managers to inform their cybersecurity risk assessment process for the 5G-enabled system. Appendix B discusses risk to cost, schedule, and performance to help program managers frame cybersecurity threats in acquisition and business contexts.

3 PROPOSED 5G SECURITY EVALUATION PROCESS

Based on its review of threat sources and knowledge of the RMF process, the study team developed the process shown in Figure 4 to guide its investigation. The process does not replace existing assessment frameworks. Rather, it can be used to guide activities in the NIST RMF system-level ***Prepare*** step for a 5G-enabled system. Because threats and vulnerabilities associated with 5G technologies may not be well known by federal system owners or information system security officers, the process helps to identify relevant threat frameworks, important 5G system security considerations, and relevant organizations and methodologies for cyber assessment of 5G systems.

5G system deployments will comprise various system elements in a wide array of configurations. Some network elements will be centralized, while others may be geographically distributed. Also, government entities may own or operate segments of the network in tandem with one or more system integrators and network operators. The intent of the system model discussed in Section 2.1 is to provide a framework that can extend and scale to describe any configuration of 5G system elements. To demonstrate a "best case" application of the security evaluation process, a notional 5G system composed of reference design elements is presented in the next subsection.

Figure 4. Proposed 5G Security Evaluation Process

3.1 Notional 5G Deployment Scenario

Many early 5G adopters in the federal government are expected to opt for a ***private*** 5G network solution that can be tailored to specific security and performance requirements in support of a mission-specific capability or application. Private 5G networks may be constructed and operated under several configurations—from a completely standalone solution (on-premises + unlicensed/shared spectrum access + government-owned infrastructure + government operator) to a "hybrid" solution that has a mix of government- and commercially-operated components and services. The example deployment presented in this document will be a greenfield, public-private hybrid implementation using network slicing, as shown in Figure 5, that uses a simple, yet realistic configuration of components, services, and actors. This notional 5G solution is not intended to serve a single mission or application. Instead, the network may be segmented to serve various applications and mission needs. It will be frequently referenced in the security evaluation process walk-through in the following sections.

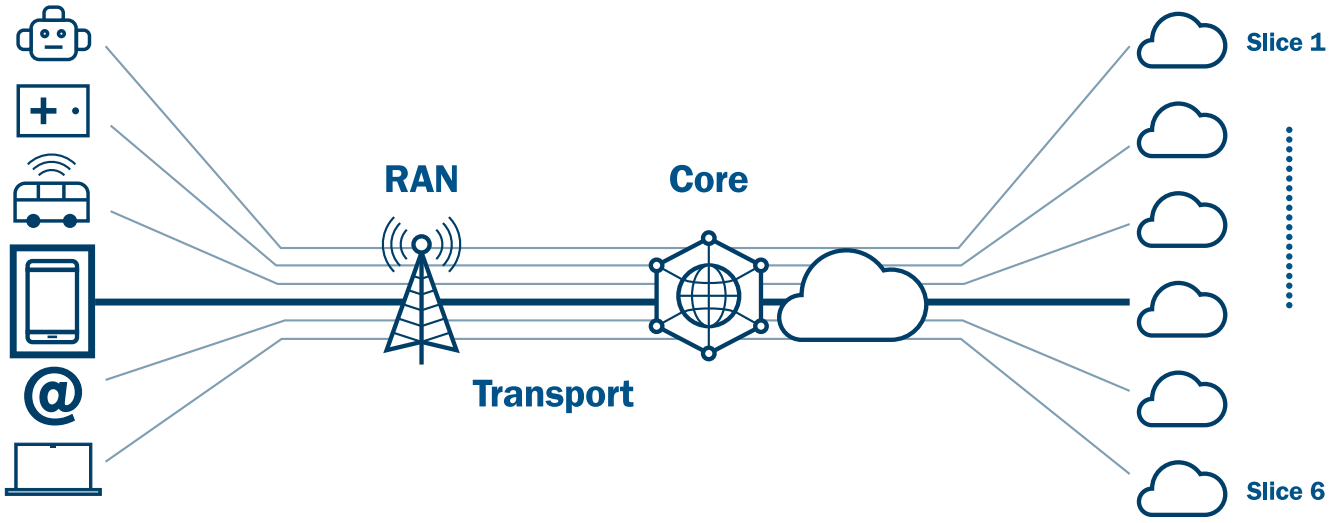

Figure 5. 5G Network Slicing Example

Key deployment details for the notional 5G deployment:

- **Network infrastructure.** The private network will be delivered by the network operator as a ***network slice*** as shown in Figure 5, which transmits through the operator's public RAN and SA core network infrastructure. The network operator will acquire, install, and maintain RAN infrastructure (including towers, base stations, and radios). The government may elect to create subnets to support multiple tenant organizations or unique application performance requirements by creating additional slices.
- **Spectrum.** The wireless segment of the private network will use the network operator's licensed spectrum offerings. Increased network capacity may be achieved with shared mid-band spectrum (e.g., Citizens Broadband Radio Service [CBRS]) for use cases that do not have high security or resiliency requirements.
- **Security.** The government must specify federal compliance and security requirements that extend beyond native 3GPP security measures and features. Also, depending on the deployment scenario and associated mission risks, each network segment may warrant additional security enhancement and remote access controls. For example, the operator may offer "end-to-end" security with its network slice offerings, however, its security capabilities may be unable to satisfy the government's security requirements and additional security mitigations may be necessary. Government-furnished smart devices will be provisioned with software-based (derived) public key infrastructure (PKI) credentials and remotely managed by an enterprise unified endpoint management (UEM) system. Integration with the government's perimeter security solution, zero trust architecture, or other wired/wireless networks and gateways may also be added at cost.
- **Network management.** Management and orchestration of the RAN segment of the network slice will be under the exclusive control of the government. Additional layers of fault, configuration, accounting, performance, and security capabilities may be applied to the RAN segment by the government or an authorized contractor.
- **Cloud computing.** The government-operated portion of this example deployment scenario does not include a MEC solution or any public cloud infrastructure or services. It is expected

that the network operator's data center(s) and edge cloud nodes execute virtualized network functions on commodity hardware.

Table 2 synopsizes the key deployment details.

Table 2. Private 5G Reference Design Elements

5G Subsystem	Selected Reference Design	Description	Site/Transmission Medium	Initial Security Measures
User Equipment	Government-Furnished Equipment (GFE) smartphones and tablets	Devices provisioned to roam between public and private networks	N/A	Derived credentials; enterprise UEM
5G RAN	Traditional (physical) RAN	RAN slice over government-owned infrastructure; no cloud-based solutions	On-premises/licensed spectrum (available shared spectrum access for extended capacity)	Network slice; "mandatory" 3GPP security measures
5G Core	Traditional public core	Network slice over a public 5G SA network	Operator's data center/fiber backhaul	End-to-end network slice; "mandatory" 3GPP security measures

The subsequent sections highlight each step of the proposed 5G security evaluation process shown in Figure 4. The example private 5G network previously defined, comprised of common 5G subsystem elements, will be used to illustrate each process step and to estimate the additional overhead incurred by deviations from the hypothetical deployment scenario. The general intent is to diminish the system complexity of ***integrating*** numerous disaggregated 5G components by ***assembling*** a handful of 5G subsystems and services that closely align to a set of technical standards. As expected, when procuring commercial off-the-shelf equipment, less customization usually equates to lower costs and faster delivery times.

3.2 Step 1: Define the Federal 5G Use Case

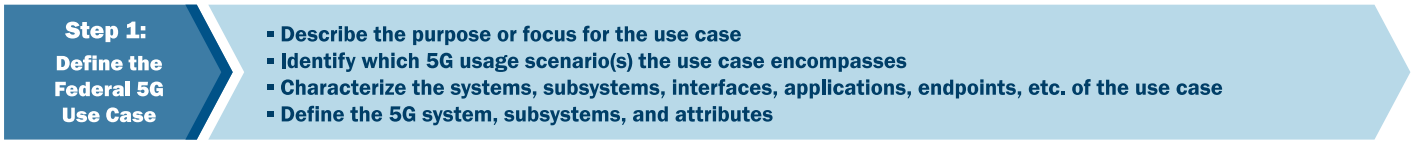

Figure 6. Step 1 Summary

The first step of the process is to define the use case and 5G usage scenario(s) (enhanced mobile broadband [eMBB], ultra-reliable low-latency communications, massive machine-type communications) it includes in the relevant 5G reference designs for UE, RAN, Core, MEC, as well as a description of interfacing systems and applications. From the use case and its associated usage scenarios, 5G system elements along with their integration with other systems and networks can be characterized. Defining the use case includes:

1. Describing the purpose for the use case (e.g., to connect devices, wearables, and environmental and building sensors to provide situational awareness for first responders).
2. Identifying which 5G usage scenario(s) the use case encompasses. Many federal use cases will take advantage of more than one of the 3GPP 5G usage scenarios.
3. Characterizing the systems, subsystems, interfaces, applications, endpoints, security, etc., that are required to support the use case.
4. Providing details of the 5G system model and reference designs discussed in Section 2.1 and interfaces to other systems, networks, or applications.

Using the example private 5G network presented in Section 3.1, the following descriptions apply for each of the key points mentioned in the first step of the process:

- **Purpose:** To deliver secure and resilient wireless communications to one or more government organization, facility, and enterprise system.
- **Usage scenario:** Private mobile network with eMBB capability to serve multiple organizations, mission needs, and applications.
- **System elements:** Traditional 5G SA Core, RAN, and UE subsystems with an end-to-end network slicing solution provided by the network operator. No network function disaggregation or virtualization. No cloud/edge processing nodes.
- **Use case configuration:** Common, traditional subsystems selected for the Core, RAN, and UE elements.

Because the example network deployment scenario represents a simplified and best-case scenario, the following alternative deployment scenarios detail potential impacts on the security evaluation process:

- **Turnkey Private 5G Network.** Hyperscale cloud providers are rapidly advancing an emerging market: private 5G networks delivered as a managed service. These services include preconfigured network equipment and management system software that can be rapidly installed to run over licensed spectrum and shared mid-band CBRS spectrum (available in the United States only). Use of such a managed service may not simplify or reduce the level of effort needed to evaluate the individual equipment (including SIM cards) and software components that comprise the packaged bundle, but it is expected to rapidly expedite deployment of the network.
- **Neutral Host Network (NHN).** To reduce excessive capital expenses and operating expenses, government sites with multiple tenant organizations may choose to share RAN infrastructure costs and outsource network operations to a qualified third party. A neutral host will enable multiple organizations and users to share networks (to potentially include sharing of the RAN and core network). Because the network equipment and possibly the spectrum will be shared, the hardware footprint and infrastructure investment may be significantly reduced. Consequently, such a NHN deployment would result in a simpler—and possibly faster—security evaluation process. This approach likely will involve additional stakeholders and increased administrative overhead (e.g., memorandums of understanding and split charging and billing).

3.3 Step 2: Identify the Assessment Boundary

Figure 7. Step 2 Summary

The complexity of 5G technology makes the process of defining the security assessment boundary for a Federal ATO difficult. Step 2 involves defining the boundary to identify the technologies and systems requiring A&A, considering ownership and deployment of the products and services that comprise the use case, and defining roles and responsibilities for implementation, management, and monitoring of security capabilities. After defining the assessment boundary, it is possible to identify the security requirements to be addressed by A&A activities. The boundary includes all components of a system to be authorized for operation and excludes separately authorized systems to which the system is connected. Boundary examples include the following elements:

- Single boundary (e.g., standalone private network).
- System-of-systems (e.g., shared network infrastructure with constituent/tenant systems).
- Hybrid (public and private).

As the example private 5G network is presently defined, the assessment boundary is evident. The bulk of the public core network resides in the network operator's data center and the network traffic is segmented via the end-to-end network slice. Unique security requirements may justify a detailed evaluation of the core network elements, processes, and suppliers. Otherwise, the assessment boundary may include the operator-provided network slice, the infrastructure buildout and operation of the government-operated RAN segment, and the endpoint devices.

However, if one of the government tenant organizations is assigned a subnet of the government's network slice, that organization may procure a MEC node to supply extra processing close to the network edge. The installation of a MEC will introduce threat vectors that will also warrant security evaluation. If the third-party MEC solution comes with its own management system, it also will be included in the assessment.

3.4 Step 3: Identify Security Requirements

Figure 8. Step 3 Methodology

Step 3 is a multi-phase step that includes conducting a high-level threat analysis of each 5G subsystem and identifying cybersecurity requirements to be addressed by A&A activities. It requires a thorough understanding of the use case under consideration to give context to the technologies employed within the assessment boundary and all interfaces to external systems. This step includes conducting a threat analysis and risk assessment as defined in the RMF system-level ***Prepare*** step. At this point in the process, the focus is on individual 5G system elements and 5G-connected systems.

To simplify mapping to requirements and assessment policies and guidance, security capabilities to mitigate the types of threats summarized in Section 2.3 have been grouped into categories. For example, authentication, authorization, and least-privilege access control are grouped under an Identity, Credential, and Access Management (ICAM) category while intrusion detection, network segmentation, and ports/protocols security are grouped under a network security category. (See Appendix B for a description of the security capability categories. Another reference for security requirements is NIST's preliminary draft of 5G cybersecurity guidance [13].)

3.4.1 User Equipment

Using the private 5G network example, the GFE smart devices are network endpoints subject to an array of threats from actors internal and external to the government's private 5G network. As GFE devices are pre-evaluated for security risks and vulnerabilities, this step is largely completed for devices that are fully compliant and up-to-date on security protections. GFE smart devices are provisioned with endpoint security protection, managed by an enterprise device management system and authenticated using Personal Identity Verification (PIV) or Common Access Card (CAC) credentials or software-based (derived) credentials. The application of these security capabilities—in accordance with agency guidance—allows these GFE devices to be immediately available for use on the government 5G network.

If non-GFE smart devices are introduced to the private 5G network, a thorough evaluation of the applicable hardware, ICAM, application, data, and communication security requirements will be necessary.

3.4.2 5G Radio Access Network

Depending on the system assessment boundary and configuration, the 5G RAN infrastructure may include infrastructure elements from one or more geographical locations and involve a variety of network switch/router, base station, and access point/cell site equipment and software.

The example private 5G network involves an on-premises RAN segment with RAN slicing to support multiple tenant applications. All hardware and software components, including cloud/edge platforms and internal and external system interfaces, are subject to the threat and security capability analyses. Certain security conditions and assurance requirements may call for a broader investigation, potentially involving Tier 2 (and beyond) vendors and proof of integrity accompanying each software bill of materials.

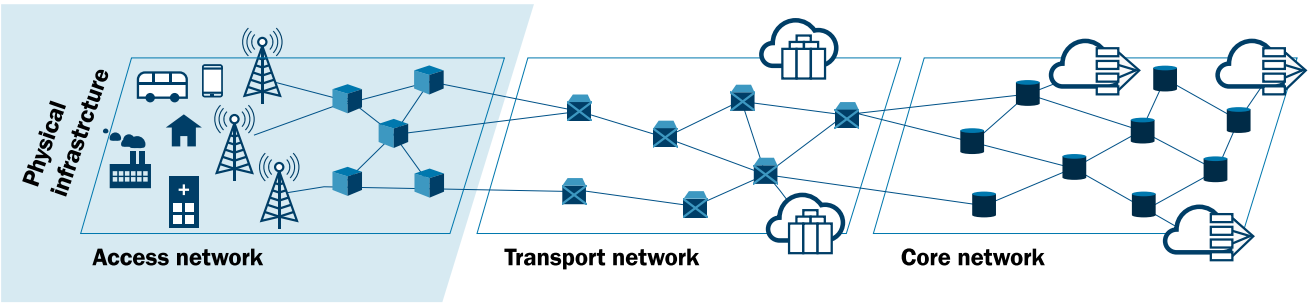

Figure 9. 5G Radio Access Network

If the RAN segments adopt an open, disaggregated RAN solution, additional Tier 1 vendors (and their component hardware and/or software products) would be involved in this security evaluation step as compared to a traditional RAN solution. The level of interoperability and penetration testing would likely increase as would the identification and mitigation of potential open RAN attack vectors.

3.4.3 5G Core Network

The 5G Core is the heart of the 5G system [14]. It connects end users to the services offered by the network by means of reliable and secure connectivity. Essential functions provided by the 5G Core include authentication and authorization of users, data connectivity, mobility management, subscriber data management, and policy management and controls.

Depending on the operator's network slicing implementation, this segmentation technique may mitigate certain aspects of the core network's evaluation—for example, exposure to certain 5G Core security and supply chain threats. However, further testing is prudent since network slicing is a new technology and its threat vectors are not yet fully understood.

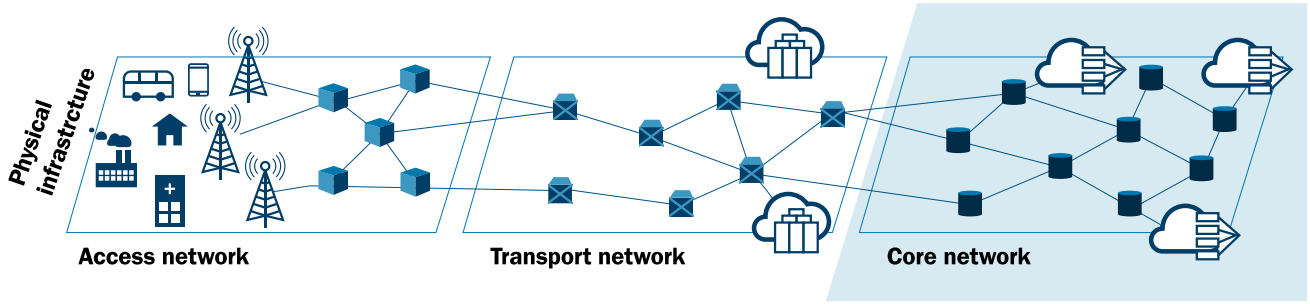

Figure 10. 5G Core Network

If shared spectrum access (e.g., CBRS) is incorporated into the private 5G network, extra measures will need to be taken to secure the proper commercial operator licensing as well as proper traffic management to ensure that high-assurance traffic remains on the licensed spectrum portion of the network [15]. Additional measures may be required upon review.

3.4.4 Deployment Environment and Operational Responsibility Considerations

A system is often more than the sum of its parts. This is the case when evaluating individual 5G system elements. There are additional security requirements and considerations that influence the overall assurance of the end-to-end system. When attempting to identify security requirements, it is also important to understand the intended deployment environment for the technologies involved and who will own and operate the associated systems. For example, attributes of the deployment environment may introduce additional risks or mitigations that could significantly impact the network's security posture. In cases where the base station equipment is located on government premises, physical access will likely be restricted to authorized government and contractor personnel. If site-specific or deployment-specific attributes are accepted as system security capabilities, these attributes will be included in the assessment boundary.

Also, as subsystem owners and operators adhere to their operations and maintenance policies, the system-level security evaluation must determine if any new vulnerabilities are introduced. If a system

is built for the government to exclusively own and operate, government cybersecurity requirements will apply.

Table 3 details the variation in security requirements associated with these procurement models.

Table 3. Deployment Environment and Security Requirements

5G System Element	Deployment Environment	Security Capability Requirements
Procurement Scenario: Build a Private 5G System for the Government		
gNB-Macro Cell	On-premises/Continental United States (CONUS)	Supply chain, access control, encryption
Small cell	On-premises/CONUS	Supply chain, access control, physical security
Network slicing	On- and off-premises (end-to-end)	Access control, isolation, virtualization
UE	N/A (mobile)	National Information Assurance Partnership (NIAP) protection profile, mobile device management, encryption
Procurement Scenario: Provision a Turnkey 5G System for the Government from an MNO		
Mobile Network	Off-premises	In accordance with contract terms, user agreements, service level agreements, commercial standards and practices, proprietary security solutions

3.5 Step 4: Map Security Requirements to Federal Guidance and Industry Specifications

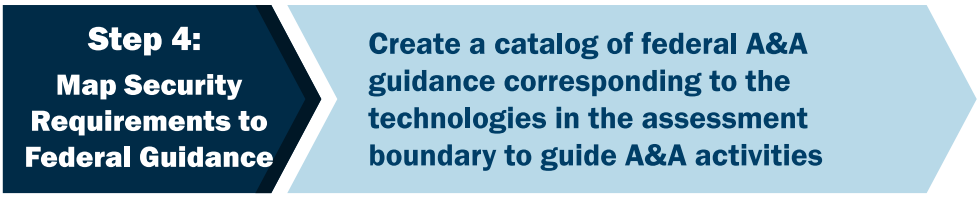

Figure 11. Step 4 Summary

Federal security requirements extend beyond those enumerated in international industry specifications. Step 4 involves the creation of a catalog of federal security A&A guidance that corresponds to the technologies included in the assessment boundary and the implied security capabilities identified in Step 3. Examples include the RMF, which applies to all categories of security capabilities, and other NIST and DoD cybersecurity guidance relevant to ICAM, supply chain risk management (SCRM), data security, virtualization/cloud/container security, and network security protection. Federal systems may be required to comply with auditable security capabilities identified for the following:

- **SCRM** as defined by acquisition policies, Executive Orders, and National Defense Authorization Acts, and Executive Order 13556, Controlled Unclassified Information.
- **RMF** as defined by NIST SP 800-37 [2], NIST SP 800-53A [16], and DoD Instruction 8510.01 [17].

- **Federal Information Processing Standards** (FIPS) as defined by FIPS 199 [18], FIPS 200 [19], and FIPS 140-2/3 [20].
- **System Hardening** as defined by organization-specific policies and/or security guidance defined by Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) [21] and NIAP Common Criteria and Protection Profiles [22].
- **Architectural Constructs** such as those defined by organizational zero trust reference architectures and adopted principles or NIST SP 800-207 [23].
- **Roots of Trust** as defined by federal or DoD PKI and ICAM policies.
- **5G Infrastructure Security Guidance** as articulated in the joint National Security Agency (NSA)-CISA publication series [24].
- **Continuous Diagnostics and Mitigation** programs such as those defined by DHS or NIST SP 800-137 [25].

Commercial service providers may be required to comply with the Federal Acquisition Regulation or Defense Federal Acquisition Regulation Supplement, NIST SP 800-171 [26], DoD's CMMC, or the Federal Risk and Authorization Management Program (FedRAMP) or DoD FedRAMP+ Cloud services.

3.6 Step 5: Assess Security Guidance Gaps

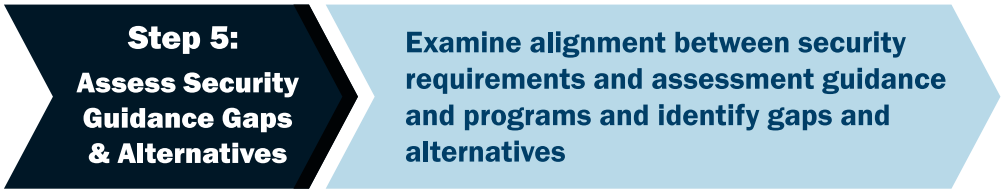

Figure 12. Step 5 Summary

Step 5 examines the alignment between security capabilities and available federal security guidance to guide A&A activities. If security capabilities are required to mitigate identified threats and reduce risk to the federal enterprise, there must be a means to assess the effectiveness of their implementation. Agency-specific policy or general government guidance or policy may be applied and/or independent assessment organizations may be established to perform assessments. Where a security requirement exists without assessment guidance, policy, or organization to verify its effectiveness for government operations, a gap is revealed. A gap also can occur when a security requirement is believed to exist to mitigate a threat, but no formal requirement has been established.

In the absence of a U.S. government assessment program or cognizable government standard, risk managers may be able to identify alternative assessment regimes, such as industry certifications, security assurance programs created by commercial or trade groups, or other best practice assessment frameworks. However, before attempting to use an assessment substitute, risk managers should carefully evaluate the suitability and comprehensiveness of any such approach.

For example, when examining 5G-enabled IoT device security, it is noted that no NIAP common criteria protection profile currently exists to guide security implementation or against which to perform security assessments. After a reasonable evaluation, an agency may find that an existing industry certification program may serve as a suitable assessment substitute.

Some gaps were discovered through preliminary analysis during this study. Also, the study team anticipates that additional threats may be identified as 3GPP, the European Telecommunications Standards Institute, and the O-RAN Alliance continue to work on study items and security specifications.

4 CONCLUSION

5G networks are designed to provide security improvements over 4G. However, the complexity of 5G networks—with new features, services, and an anticipated massive increase in the number and types of devices 5G will serve, coupled with the use of virtualization and disaggregation of the RAN and the 5G Core—expands the threat surface and makes it challenging to define the system boundary. Federal enterprises implementing—or planning to implement—5G-enabled systems may not be aware of how inclusion of 5G technologies impacts the system risk assessment/ATO process. Additionally, with deployment of 5G in early stages, federal enterprises may not have awareness of potential threats to 5G and ready access to the security capabilities that 5G offers.

To determine how inclusion of 5G technologies in a federal system might impact the ATO process, the study team developed the proposed five-step 5G Security Evaluation Process as presented in this document. The 5G Security Evaluation Process identifies important threat frameworks, 5G system security considerations, industry security specifications, federal security guidance documents, and relevant organizations and methodologies for cyber assessment of 5G systems. The study team also identified—and presented in this document—potential gaps in existing security guidance for some new 5G features and services.

From its investigation, the study team concluded that the ***NIST RMF is technology-neutral and does not need to be modified for 5G***. The proposed 5G Security Evaluation Process described in this document is a repeatable methodology that federal program/project managers can use as they conduct the ***Prepare*** step of the NIST RMF for a 5G-enabled system. It can be applied to a wide array of 5G system architectures, deployment scenarios/use cases, and operational environments.

APPENDIX A: REFERENCE DESIGNS

Category	5G Reference Design	Description
5G UE	Smart device	The set of UE elements and attributes supporting a smart device such as a smartphone or tablet.
5G UE	IoT, Cyber physical system (CPS)[1] [2] device	The set of UE elements and attributes supporting an IoT or CPS device, including monitoring devices (e.g., sensors), reader/scanner devices, controls, and gateway/hub devices that may aggregate multiple devices into 5G access network communication. Examples include smart grid, autonomous automobile systems, industrial control systems, robotics, and unmanned aerial vehicles. While distinctions can be made between IoT and CPS devices, there are more commonalities and convergence of definitions that can be leveraged as a basis for security evaluation.
5G RAN	5G System with Traditional RAN	The set of RAN elements and attributes supporting deployment in a "traditional" baseband unit (BBU). Typically, this is a bare metal RAN solution with proprietary fronthaul interface to the Radio Unit. Interfaces internal to BBU may also be proprietary.
5G RAN	5G System with Virtual/Cloud RAN	The set of RAN elements and attributes supporting deployment in a cloud or virtual environment. Disaggregation between the central unit and distributed unit is common following 3GPP specifications.
5G RAN	5G System with Open RAN (O-RAN)	The set of RAN elements and attributes that support an Open RAN deployment following O-RAN Alliance architecture and interfaces.[3]
5G Core	5G System with Private Core	The set of Core elements and attributes supporting deployment as a Private Core network, isolated from MNO-provided (public) 5G network functions.

[1] NIST. Cyber-Physical Systems and Internet of Things. NIST SP 1900-202. March 7, 2019. https://www.nist.gov/publications/cyber-physical-systems-and-internet-things.

[2] Examples of CPS include smart grid, autonomous automobile systems, industrial control systems, robotics systems, and automatic pilot. Khaitan et al., "Design Techniques and Applications of Cyber Physical Systems: A Survey," IEEE Systems Journal, Vol. 9, Issue 2, 2014. https://ieeexplore.ieee.org/document/6853346.

[3] O-RAN ALLIANCE. Accessed April 30, 2022. https://www.o-ran.org/.

Category	5G Reference Design	Description
5G Core	5G System with Public Core	The set of Core elements and attributes supporting deployment as a Public Core network as part of an MNO-provided (public) 5G network.
MEC	Private/Enterprise Edge	The set of MEC elements and attributes supporting deployment of a privately owned and managed MEC independent/isolated from an MNO network.
MEC	Public Edge Cloud	The set of MEC elements and attributes supporting deployment of a MEC in an edge cloud environment from an MNO or public cloud provider. In this case, the MEC is not provided or managed by the enterprise.

APPENDIX B: 5G SECURITY RISKS FOR PROGRAM MANAGERS

Technical discussions about 5G vulnerabilities and mitigations may be difficult to frame in acquisition or business terms such as impacts to cost, schedule, and performance. As a result, disconnects and delays often ensue as security requirements are formulated, embedded into contracts, and evaluated throughout the system's lifecycle.

Risks such as those discussed in Section 2.3 are generally viewed as a function of probability of occurrence and impact to the mission or operation. Some serious threats may be considered low risk because they are unlikely to occur. Conversely, nominal 5G threats may demand attention and mitigation resources due to their high-impact potential and frequency. Unfortunately, such determinations cannot be made in advance because each 5G deployment scenario introduces a unique set of vulnerabilities and mitigations. However, there are some common risk attributes that can help frame many cybersecurity threats in acquisition and business contexts in advance of a 5G network's risk assessment.

Let us begin with the major 5G subsystems (i.e., the 5G Core, RAN, MEC, and UE):

- The **public 5G Core** network will likely reside in a commercial data center that has high-speed internet connectivity, significant computation and storage resources, power and cooling redundancy, and physical security protections. As with most data centers, this facility is linked with other geographically distributed sites to provide near-instant failovers in the event of a physical or cybersecurity attack, a widespread network failure, or a catastrophic natural event. As the 5G Core functions are evolving from bespoke hardware to disaggregated, virtualized functions, they are becoming increasingly susceptible to compromise as any networked asset. To date, cloud and data center security advancements largely have mitigated known attack vectors from external low to mid-level cyber criminals. Following are additional 5G Core considerations:
    - **Costs.** Additional security measures may be requested—at cost—for implementation in the vendor-provided core network, but if any resources are available to strengthen the 5G network's security posture they should be applied in the RAN segment of the network (in most cases). However, above-baseline services (e.g., enhanced reporting or split billing) may incur additional costs to implement.
    - **Schedule.** A benefit of the public 5G Core evolving into multiple service-oriented, cloud-native applications is the speed of delivery. For instance, new service requests or service changes may be rapidly implemented by the system owner, cloud service provider, or network operator. There are little to no prominent schedule risks.
    - **Performance.** Depending on several factors, additional security measures may result in degraded capability and/or network performance. The tradeoff between the incurred cost of additional security protections and the likelihood of lost performance, capability, or value should be considered by all stakeholders.
- For **private 5G** solutions with a government-operated core network, it is recommended that a data center with comparable resiliency and security measures is used for 5G networks supporting high-assurance applications and data. Existing government-wide acquisition contracts are available to aid in the selection of trusted 5G vendors, products, and services.

- The **RAN** segment of the 5G network may be the most difficult subsystem to address from a risk perspective. There are multiple configurations and deployment scenarios that can greatly influence the RAN's threat surface. In addition to the usual assortment of network equipment and software, the RAN segment also includes the air interface that is subject to various forms of eavesdropping and jamming attacks. Some of the RAN components may be publicly accessible (e.g., small cells positioned atop lamp posts and buildings) and hence may be illegally accessed, stolen, or damaged.
  The 5G RAN is evolving to include more automation (via embedded AI/ML algorithms) and virtualization (via software-defined networking and network functions virtualization). With each phase of technological evolution, additional compute, connect, and storage elements will be needed. Following are additional RAN considerations:
    - **Costs.** Cost risks are largely unknown as large-scale public sector deployments are still in the operational testing and evaluation stages. Depending on the 5G architecture (SA versus NSA), existing RAN infrastructure may be reused, thereby reducing construction and installation costs and minimizing schedule delays.
      If network slices are created, assigned, and managed by government personnel or federal contractors, then additional service contracts may not be necessary. For deployments that serve multiple sites and tenants, additional costs for technical and administrative support services may be requested. Significant costs may be incurred as the government requests custom and/or complex RAN security features and configurations.
    - **Schedule.** Schedule delays are possible, particularly for disaggregated, multi-vendor RANs. With any significant change or update to a system component or interface, a round of integration and security testing will be required. Depending on the vendor(s) and component(s) involved, a supply chain assessment may also be a procurement prerequisite.
    - **Performance.** As previously stated, the RAN segment is capable of myriad configurations (often referred to as "functional splits") to achieve a combination of performance and cost objectives. Network performance also will be dependent upon changes to signal strength, capacity, latency, and interference. With each selected configuration and spectral profile, end-to-end network performance may vary in throughput level and consistency.
- A public edge cloud may comprise one or more **MEC** nodes that host added computation and storage closer to network endpoints. Operators may configure and locate a MEC solution to satisfy specific performance and latency requirements. MEC nodes inherit many attributes of traditional cloud computing nodes. Consequently, many of the cloud computing risks and mitigations stated earlier in the 5G Core section will likely apply. Following are additional MEC considerations:
    - **Costs.** Custom MEC solutions and supporting services are offered by MNOs, system integrators, hyperscale cloud providers, and managed service providers. Planning, design, and implementation costs will vary according to regulatory constraints and

customer requirements such as system integration requirements, coverage, requested features, and security options.

- **Schedule.** Schedule risks are possible as the addition of MEC nodes may add to the number of overall testing, assessment, and regulatory activities. These additional activities may include cybersecurity and supply chain risk assessments; platform, vendor, and/or product certification; and integration, security, and performance testing. In cases where an MEC deployment is located outside of the government system owner's property line or sphere of control, legal or regulatory activities may incur schedule delays.
- **Performance.** Depending on the application, the addition of one or more MEC nodes may result in significant performance improvements. Because the scale and density of the edge cloud infrastructure may vary, so may the performance improvements per application. Also, since the compute and storage platform(s) may be subject to frequent upgrades, the MEC system architecture should employ standardized external interfaces and APIs whenever possible.

- In many instances, the **UE** is the most accessible and vulnerable 5G subsystem. The UE is often the network endpoint and hosts user and enterprise applications and data (including sensitive and/or Personally Identifiable Information [PII]). Even with deployment of various forms of endpoint security (e.g., encrypted VPN and local memory, antivirus, and firewalls), UEs are highly susceptible to both malicious and non-malicious actions (e.g., human error or misconfigurations). GFE smartphones and tablets have completed security testing and are typically provisioned with enterprise security measures to mitigate known attack vectors. Additional security features and mitigations may be enacted via user (e.g., acceptable use agreements) or organizational (e.g., disable location tracking) policies. Following are additional UE considerations:
  - **Costs.** GFE smartphones and tablet devices are typically bundled with an enterprise wireless service plan or purchased separately (e.g., Wi-Fi only). Other devices such as 5G-equipped vehicles, non-GFE smart devices, and IoT devices are subject to government security testing or an approved independent, third-party security assessment. The extent of the security assessment will be determined by several factors, including connectivity to government networks and data sources, highest classification level of applications and data, and the native security features of the host device. Discovered vulnerabilities in the application and/or firmware usually is addressed via over-the-air software updates at no additional cost to the end user or enterprise.
  - **Schedule.** Only in rare cases will a security solution severely impair device operation or performance. In the event of an impaired or bricked device, enterprise help desk support should be able to remedy the issue in a timely fashion. However, the availability of newly released UEs may be delayed due to government security testing and provisioning.

- **Performance.** Any performance issues incurred by supplementary security measures will likely be related to the network. No significant device-level performance risks are identified at this time.

APPENDIX C: SECURITY CAPABILITY DESCRIPTIONS

Application and API Security

Application and API security is the practice of developing, deploying, integrating, and monitoring security systems that defend application software, computer interfaces, and associated computing hosts. Application and API security solutions are applied to detect, protect, and respond to attacks associated with software vulnerability exploitation, malicious code injection (i.e., virus, malware, Structured Query Language), application misuse, directory traversal, and unauthorized system and data access.

Communication and Interface Security

Communication and interface security is the cybersecurity practice of implementing and monitoring network and interface security mechanisms and systems. Communication and interface security applies segmentation mechanisms to isolate network segments, computer hosts, and application and data systems. Communication and interface security may overlap with application, API, and data security due to the use of universal mechanisms in system segmentation and the protection of data through encryption. Communication and interface security may also apply ICAM, data, application, and API security mechanisms to accomplish its objectives. Communication and interface security solutions are applied to detect, protect, and respond to attacks associated with DoS, network and host traversal, and unauthorized system access.

Data Security

Data security is the cybersecurity practice of protecting data at rest, in transit, and—to the greatest extent possible given technical means—in processing. Data security tools include encryption for confidentiality protection, hashing or signing for integrity protection and actor nonrepudiation, and means for backup and recovery to ensure availability. The practice of data security involves the assessment of data sensitivity and the analysis of threats to inform the ICAM practice regarding the implementation of fine-grained, role-based, least privilege access control policies and mechanisms, which may be dynamic and informed by trust scoring. The data security practice may also involve the tagging of data for sensitivity and discovery purposes and the negotiation of data use agreements. It also is responsible for compliance with privacy-related regulations on PII and Protected Health Information. Data security solutions are applied to protect, detect, and respond to attacks associated with unauthorized access, data modification or deletion, statistical data resolution, and DoS threats.

Hardware/Firmware Security

Hardware and firmware security is the practice of building, configuring, hardening, and maintaining the base computing platforms intended for application, data, and computation system hosting. The hardware security practice may involve the implementation and management of mechanisms designed to prevent side-channel leakage as well as system tampering. The firmware security practice typically involves the implementation, update, and maintenance of base computer hardware basic input/output systems, operating systems, security storage, and Trusted Platform Module components. Hardware and firmware solutions are applied to protect against attacks associated with hardware and firmware vulnerabilities, side-channel leakage, device spoofing, and computation integrity threats.

Identity, Credential, and Access Management

ICAM is the cybersecurity practice involving the identification of entities (users and devices); the assignment of system and data access credentials (IDs, passwords, certificates, multifactor authentication components [e.g., CAC/PIV, soft-certs, hard tokens]); assignment of access-related roles, attributes, rights, and privileges; and the life-cycle management of these elements to include revocation and revision. Considering Zero Trust Architecture principles, associated processes may be automated and dynamic in response to threat intelligence and measures of risk, and trust scoring may be used to inform access control decisions. The ICAM practice is responsible for the implementation and management of access control policy and enforcement mechanisms including Credentialing, Active Directory, Local Directory Access Protocol, and Zero Trust Policy Enforcement Point and Policy Decision Point systems. ICAM solutions are applied to detect, protect, and respond to attacks associated with unauthorized access, identity fraud, privilege escalation, and insider threat.

Information Technology (IT) Operations and Monitoring

IT operations and monitoring is the practice of tracking system inventory, maintaining the configuration management database, operating and maintaining systems, supporting user services, implementing security information and event management systems, developing cyber analytics for threat detection, and detecting and responding to cybersecurity intelligence and events. It includes the practice of Continuous Diagnostics and Mitigation, information systems continuous monitoring, cybersecurity incident response and recovery, disaster recovery, and continuity of operations planning. IT operations and monitoring solutions are applied to detect, protect, and respond to attacks associated with network intrusion, malicious code injection, ransomware, eavesdropping, DoS, and unauthorized access threats.

Network Security

Network security is the practice of building, configuring, and monitoring network and network security systems and responding to network security events. Network security employs ICAM, network segmentation, intrusion detection and protection, firewalls, and encryption technologies to protect network systems. Network security solutions are applied to protect, detect, and respond to attacks associated with network intrusion, DoS, rogue device access, unauthorized access, eavesdropping, and network traversal threats.

Physical and Environmental Security

Physical and environmental security controls and protects access to systems and maintains vital plant systems necessary to maintain IT operations. Physical security may involve the development of secure facilities, credentialing of personnel having physical access, and management of access policies and policy enforcement systems, as well as monitoring and escorting of personnel. Environmental security involves the monitoring and maintenance of plant utility systems (e.g., power, water), fire and safety systems, heating and air conditioning, and backup systems. Physical and environmental security practices may employ ICAM systems for identity and credential management as well as network, application, and data security practices for the protection of physical plant Industrial Control Systems, Supervisory Control and Data Acquisition, and IoT devices. Physical and environmental security solutions detect, protect, and respond to attacks associated with unauthorized

physical access to systems and data, DoS, and threats from natural disasters, power outages, and failure of equipment or controls due to circumstances that exceed expected operating parameters.

Resiliency

Resiliency is the engineering practice of implementing systems that can withstand cybersecurity attacks and natural disasters. Its primary goal is to maintain IT system availability and ensure continuity of operations. Resilient system design approaches can include redundant systems, deception techniques, over-provisioning of systems, non-persistence, automation in systems maintenance, and reliance on Cloud Service Provider (CSP) systems availability. Resiliency solutions detect, protect, and respond to attacks associated with DoS, ransomware, loss of data, and natural disasters.

Security of AI/ML Implementation

AI/ML security is the practice of developing and implementing systems to protect the computation and integrity of AI/ML data. AI/ML systems may involve the aggregation of large and rapidly streaming data sources. As such, data, communication, and network security practices may be involved as well as ICAM practices to control access to AI/ML systems. Application, data, communications, and interface security practices may also be employed to control access to AI/ML system capabilities and data as well as cryptographic approaches to data integrity hashing and signing to facilitate the identification and use of trusted data. AI/ML security solutions protect, detect, and respond to cybersecurity attacks associated with unauthorized access, DoS, malicious code injection, and data spoofing threats.

Supply Chain Risk Management

SCRM is the practice of monitoring and managing risks associated with material builds of hardware and software used for systems implementation. It involves the testing and inspection of systems for the identification and mitigation of supplier-embedded vulnerabilities or vulnerabilities resulting from the integration of supplied components or poor development practices. SCRM mechanisms may include supplier risk assessment, hardware visual inspection, and software vulnerability and penetration testing as well as the quantification of risk to inform risk management decisions. SCRM solutions are applied to protect, detect, respond to, and manage the risk of attacks associated with malicious or vulnerable components embedded in systems, malicious code injection, and vulnerable system threats.

Virtualization/Cloud/Container Security

Virtualization, cloud, and container security protects systems and resources that have been abstracted to efficiently service a multitude of compute workloads, applications, and users. It leverages resource pooling and multi-tenant technologies to provide access to systems and services aggregated to serve a common purpose to commoditize costs. Though clouds can be open to the public or limited to private consumer usage, CSP systems are generally based upon virtualization, the delivery of VMs and supporting services, and multi-tenant segmentation and orchestration technologies. At the heart of virtualization technology is the virtualization platform, which may host an array of VMs operated by one or many authorized tenants sharing a common set of abstracted hardware resources. Container security leverages the virtualization platform by further abstracting operating systems to the most reduced set of executables necessary to host a particular application.

Container systems run on a cluster of VMs and provide an inherently reduced threat surface due to their reduced instruction set. The use of cloud services typically implies the presence of a shared security responsibility model in which cybersecurity threats and mitigations are performed cooperatively between the consumer and the CSP. Multi-tenant security solutions involve account and resource isolation through inherent virtualization platform capabilities, but may also include ICAM, network, data, application, API, and communication and interface security technologies and practices. Because of the possible existence of unknown adversaries in the multi-tenant environment, an organization may choose private cloud environments or request reservation of individual hardware platforms for hosting sensitive workloads in a public cloud. Since virtualization allows the deployment of systems using scripts for automation, organizations have implemented Development, Security, and Operations (DevSecOps) pipelines that integrate Infrastructure as Code (IaC) capabilities. IaC-enabled DevSecOps pipelines typically employ SCRM and other vulnerability and system hardening methods to ensure trusted VM, container, and cloud service deployment. Virtualization, cloud, and container security solutions are applied to protect, detect, and respond to attacks associated with DoS and unauthorized access to cloud resources or data.

APPENDIX D: NETWORK SLICE SECURITY

End-to-End Network Slice Security (UE, RAN, Core, Orchestration)

Network slicing is introduced to cellular technology in 5G. As a new technology, there is no government policy or guidance to specify its security capabilities to meet government security requirements. A Network Slice is defined as a logical network that provides specific network capabilities and network characteristics. Additionally, a Network Slice instance is defined as a set of Network Function instances and the required resources (e.g., compute, storage, and networking resources) that form a deployed Network Slice. A Network Slice instance contains at least one virtual network function. There is no government security guidance for the security capabilities of 5G virtual network functions—and by extension—no federal security guidance for network slicing.

An end-to-end slice is from the UE via the RAN, transport network (e.g., backhaul), and the core network. The security capabilities for each end-to-end network slice segment are different. There is also management and orchestration associated with provisioning the end-to-end slice (including preparation with network slice template, commissioning, operation, and decommissioning). There is a gap in guidance to address how all these segments work together as a cohesive slice with all the required security capabilities; inter- and intra-slice isolation must be addressed. Slice isolation includes the following aspects:

- Isolation of traffic: the slices should ensure that data flow of one slice does not move to another.
- Isolation of bandwidth: slices should not use any bandwidth assigned to other slices.
- Isolation of processing: while all virtual slices use the same physical resources, independent processing of packets is required.
- Isolation of storage: data related to a slice should be stored separately from data used by another slice.

Zero Trust Architecture Principles

Zero trust is the guiding principle for mitigating network slicing threats. For example, zero trust can be leveraged to prevent unauthorized access of another slice from a slice with weaker security. It also can be used to prevent a DoS attack (i.e., a slice with weaker security and performance requirements consumes all the shared resources, thus affecting a DoS attack on a slice with more stringent security and performance requirements).

Bibliography

[1] Federal Mobility Group, "Framework to Conduct 5G Testing," November 2020. [Online]. Available: https://www.cio.gov/assets/files/Framework-to-Conduct-5G-Testing-508.pdf. [Accessed December 2021].

[2] NIST Joint Task Force, "NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018. [Online]. Available: https://csrc.nist.gov/Projects/Risk-Management. [Accessed November 2021].

[3] NIST, "Cybersecurity Framework Version 1.1," 16 April 2018. [Online]. Available: https://www.nist.gov/cyberframework/framework. [Accessed October 2021].

[4] Department of Defense, Office of the Under Secretary of Defense, Acquisition and Sustainment, "Securing the Defense Industrial Base CMMC 2.0," DoD, 2021. [Online]. Available: https://www.acq.osd.mil/cmmc/index.html. [Accessed December 2021].

[5] MITRE, "MITRE ATT&CK," MITRE, 2021. [Online]. Available: https://attack.mitre.org/. [Accessed September 2021].

[6] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape for 5G Networks Report," 14 December 2020. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks. [Accessed October 2021].

[7] S. Rao, S. Holtmanns and T. Aura, "Threat modeling framework for mobile communication systems," May 2020. [Online]. Available: https://www.researchgate.net/publication/341310813_Threat_modeling_framework_for_mobile_communication_systems. [Accessed September 2021].

[8] 3GPP, "TS 33.501 Security architecture and procedures for 5G System," 3GPP, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169. [Accessed December 2021].

[9] FCC CSRIC, "Communications Security, Reliability, and Interoperability Council VII," FCC, 2021. [Online]. Available: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii. [Accessed October 2021].

[10] The 5G Infrastructure Public Private Partnership, "5G-ENSURE," 5G PPP, 2021. [Online]. Available: http://www.5gensure.eu/. [Accessed December 2021].

[11] GSM Association, "5G Cybersecurity Knowledge Base," GSMA, 2021. [Online]. Available: https://www.gsma.com/security/5g-cybersecurity-knowledge-base/. [Accessed November 2021].

[12] CISA, Office of the Director of National Intelligence, National Security Agency, "Potential Threat Vectors to 5G Infrastructure," 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf. [Accessed November 2021].

[13] NIST National Cybersecurity Center of Excellence (NCCoE), "5G Cybersecurity," NIST NCCoE, [Online]. Available: https://www.nccoe.nist.gov/5g-cybersecurity. [Accessed March 2022].

[14] Ericsson, "5G Core (5GC)," Ericsson, 2021. [Online]. Available: https://www.ericsson.com/en/core-network/5g-core. [Accessed December 2021].

[15] Wireless Innovation Forum, "Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band," 11 March 2020. [Online]. Available: https://winnf.memberclicks.net/assets/CBRS/WINNF-TS-0112.pdf. [Accessed December 2021].

[16] NIST Information Technology Laboratory, "SP 800-53A, Rev. 5 (Draft), Assessing Security and Privacy Controls in Information Systems and Organizations," NIST, August 2021. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/draft. [Accessed November 2021].

[17] DoD, "DoDI 8510.01, Risk Management Framework for DoD IT," 29 December 2020. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300. [Accessed March 2022].

[18] NIST Information Technology Laboratory, "FIPS 199: Standards for Security Categorization of Federal Information and Information Systems," NIST, February 2004. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/199/final. [Accessed November 2021].

[19] NIST Information Technology Laboratory, "FIPS 200: Minimum Security Requirements for Federal Information and Information Systems," NIST, March 2006. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/200/final. [Accessed December 2021].

[20] NIST Information Technology Laboratory, "FIPS 140-3: Security Requirements for Cryptographic Modules," NIST, 22 March 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/140/3/final. [Accessed December 2021].

[21] DISA, "Security Technical Implementation Guides (STIGs)," DISA, [Online]. Available: https://public.cyber.mil/stigs/. [Accessed December 2021].

[22] NIAP, "NIAP Approved Protection Profiles," NIAP, 2021. [Online]. Available: https://www.niap-ccevs.org/Profile/PP.cfm. [Accessed December 2021].

[23] NIST Information Technology Laboratory, "SP 800-207, Zero Trust Architecture," NIST, August 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final. [Accessed December 2021].

[24] CISA and NSA, "5G Security and Resilience : 5G Resources and News," CISA and NSA / ESF, 2021. [Online]. Available: https://www.cisa.gov/5g. [Accessed March 2022].

[25] NIST Information Technology Laboratory, "SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," NIST, September 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-137/final. [Accessed December 2021].

[26] NIST Information Technology Laboratory, "SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizationss," NIST, February 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final. [Accessed November 2021].

[27] NSA Central Security Service, "Commercial Solutions for Classified Program Overview," NSA, [Online]. Available: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Overview/. [Accessed November 2021].

[28] EU GDPR, "General Data Protection Regulation," Intersoft Consulting, [Online]. Available: https://gdpr-info.eu/. [Accessed December 2021].

[29] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," January 2020. [Online]. Available: http://www.nrg5.eu/wp-content/uploads/2020/02/CybersecurityofGnetworksEUToolboxofriskmitigatingmeasurespdf.pdf. [Accessed November 2021].

[30] 3GPP, "3GPP Specification Series, TS 33.511 - TS 33.522, TS 33.527," 3GPP, [Online]. Available: https://www.3gpp.org/DynaReport/33-series.htm. [Accessed March 2022].

[31] GSM Association, "Network Equipment Security Assurance Scheme (NESAS)," GSMA, 2021. [Online]. Available: https://www.gsma.com/security/network-equipment-security-assurance-scheme/. [Accessed November 2021].

[32] GSM Association, "NESAS Evaluated Network Equipment Products," GSMA, 2021. [Online]. Available: https://www.gsma.com/security/nesas-evaluated-network-equipment-products/. [Accessed November 2021].

[33] O-RAN Alliance, "Testing & Integration of O-RAN solutions," O-RAN Alliance, 2019. [Online]. Available: https://www.o-ran.org/testing-integration. [Accessed December 2021].

[34] CTIA, "Internet of Things (IoT) Cybersecurity Certification," CTIA, 2021. [Online]. Available: https://ctiacertification.org/program/iot-cybersecurity-certification/. [Accessed November 2021].

[35] European Union Agency for Cybersecurity, "Securing EU's Vision on 5G: Cybersecurity Certification," ENISA, 23 February 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification?msclkid=75c076b3ba7211ec9507574a90ea9344. [Accessed March 2022].

[36] ENISA, "Cybersecurity Certification: Candidate EUCC Scheme V1.1.1," ENISA, 25 May 2021. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1. [Accessed January 2022].

ACRONYMS

Acronym	Definition
3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
A&A	Assessment and Authorization
AI	Artificial Intelligence
API	Application Programming Interface
ATO	Authorization to Operate
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BBU	Baseband Unit
CAC	Common Access Card
CBRS	Citizens Broadband Radio Service
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CNF	Cloud-Native Network Function
CONUS	Continental United States
CPS	Cyber Physical System
CSF	Cyber Security Framework
CSP	Cloud Service Provider
CSRIC	Communications Security, Reliability, and Interoperability Council
CU	Centralized Unit
DDoS	Distributed Denial of Service
DevSecOps	Development, Security, and Operations
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoS	Denial of Service
DU	Distributed Unit (gNB)
EMBB	Enhanced Mobile Broadband
ENISA	European Union Agency for Cybersecurity
ENSURE	Enablers for Network and System Security and Resilience
EU	European Union

Acronym	Definition
FCC	Federal Communications Commission
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
GFE	Government Furnished Equipment
IaC	Infrastructure as Code
ICAM	Identity, Credential, and Access Management
IoT	Internet of Things
IT	Information Technology
MEC	Multi-access Edge Computing
ML	Machine Learning
MNO	Mobile Network Operator
NESAS	Network Equipment Security Assurance Scheme
NHN	Neutral Host Network
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NR	New Radio
NSA	National Security Agency
NSA	Non-Standalone
O-RAN	Open RAN
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RAN	Radio Access Network
RMF	Risk Management Framework
S&T	Science and Technology
SA	Standalone
SCAS	Security Assurance Specification
SCRM	Supply Chain Risk Management
SIM	Subscriber Identity Module
SP	Special Publication
STIG	Security Technical Implementation Guide

Acronym	Definition
TS	Technical Specification
US	United States
UE	User Equipment
UEM	Unified Endpoint Management
VM	Virtual Machine
VNF	Virtual Network Function