NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# 5G Cybersecurity

## *Volume A: Executive Summary*

NIST
Special Publication
1800-33A

Initial Public Draft

Michael Bartock
Jeffrey Cichonski
Murugiah Souppaya
*Information Technology Laboratory*

Karen Scarfone
*Scarfone Cybersecurity*

Parisa Grayeli
Sanjeev Sharma
*The MITRE Corporation*

March 2025

**This publication is available free of charge from: https://www.nccoe.nist.gov/publications/practice-guide/nist-sp-1800-33-ipd-5g-cybersecurity**

## Purpose and Scope

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with technology providers and other companies on a project to develop example solution approaches for safeguarding 5G networks. These solutions use combinations of cybersecurity and privacy measures drawn from 5G capabilities and recommended practices. Details of the project's goals and implementation, including its technologies and architectures, along with testbed observations and findings are being documented in a NIST Cybersecurity Practice Guide. As the first volume of the practice guide, this document summarizes the most significant cybersecurity and privacy recommendations from the other volumes. Detailed information on 5G cybersecurity and privacy capabilities is also being published as part of a white paper series.

## Audience

This volume is intended for technology, cybersecurity, and privacy professionals who are involved in using, managing, or providing 5G-enabled services and products. This includes commercial mobile network operators, potential private 5G network operators, and end-user organizations.

# Project Approach Overview

## The Challenge

Fifth-generation technology for broadband cellular networks – 5G – will significantly improve how humans and machines communicate, operate, and interact in the physical and virtual world. 5G provides increased bandwidth and capacity, and low latency, which will benefit organizations in all sectors as well as home consumers. However, professionals in the fields of technology, cybersecurity, and privacy are faced with safeguarding this technology while its development, deployment, and usage are still evolving. As 5G evolves, its capabilities are simultaneously being specified in standards bodies, implemented by equipment vendors, deployed by network operators, and adopted by consumers.

Current standards development primarily focuses on cybersecurity and privacy for the standards-based, interoperable interfaces between 5G components. The 5G standards do not specify protections to deploy on the underlying information technology (IT) components that support and operate the 5G system. This lack of specification increases the complexity for organizations planning to leverage 5G, who are challenged to determine what cybersecurity and privacy capabilities 5G can provide and how they can deploy these features, as well as what supplementary capabilities they may need to implement to safeguard data and communications.

## Addressing the Challenge

To address this challenge, the NCCoE is collaborating with technology providers to develop example solution approaches for safeguarding 5G networks through a combination of the following measures:

- strengthening the system's architectural components;
- providing a trusted and secure cloud-native hosting infrastructure to support the 5G Core Network functions, radio access network (RAN) components, and associated workloads; and
- enabling the cybersecurity and privacy features introduced in the 5G standards, including demonstrating how to continuously monitor 5G traffic on both signaling and data layers to detect and prevent cyber attacks and threats.

These measures support common use cases and meet industry sectors' recommended cybersecurity and privacy practices and compliance requirements. If the project identifies gaps in 5G cybersecurity and privacy standards, the appropriate standards development organizations (SDOs) will be notified, and some of the project's collaborators may contribute to SDO efforts to address the gaps.

Given the evolution of the standards, the availability of commercial products, and the alignment with commercial networks, the project focuses on 5G standalone (SA) networks, which can support 3GPP standards-based 5G cybersecurity and privacy enhancements that 5G non-standalone (NSA) networks cannot.

# Key Recommendations

Here are key recommendations based on observations and findings from the portions of the NCCoE project that have been performed so far. Additional key recommendations are expected to be added in subsequent drafts.

1. **Design and operate 5G systems' complex cloud technology stacks so they support advanced cybersecurity and privacy capabilities and design principles.** For example, including hardware roots of trust in the stacks can aid in assuring the integrity of the stacks' hardware, firmware, and software configurations. Enabling such protections in the supporting infrastructure will help ensure that 5G networks are protected against advanced cyber attacks. Appropriate monitoring capabilities can provide visibility and useful information for prompt detection, response, and recovery from cyber attacks. The NCCoE project describes these cybersecurity and privacy capabilities, implements them in real-world commercial equipment, and demonstrates how they protect 5G networks and subscribers.
2. **Enable and properly configure the optional, standardized 5G cybersecurity and privacy features specified by 3GPP.** 5G networks are complex systems of systems often designed and deployed in a one-off fashion. Each 5G network will have unique attributes to meet requirements, make efficiencies, best leverage existing capabilities, and be shaped by spectrum resources. Simply speaking, no two public 5G networks are the same. However, many cybersecurity and privacy capabilities that protect 5G networks and their users are available to all 5G networks regardless of technical implementation specifics. Enabling these capabilities and configuring them properly will enhance the cybersecurity and privacy of systems and subscribers. NCCoE is publishing a white paper series to cover capability-specific configurations.

> While the NCCoE is using a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best fit your organization. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

# Related Resources

## NCCoE 5G Cybersecurity Resources

- NCCoE 5G Cybersecurity Project Website
- Project Description (*5G Cybersecurity: Preparing a Secure Evolution to 5G*)
- December 2023 webinar on the project
- 5G Cybersecurity Practice Guide Volume B: *Approach, Architecture, and Security Characteristics* (SP 1800-33B, preliminary draft) is for **technology, cybersecurity, and privacy program managers and staff** who are concerned with how to identify, understand, assess, and mitigate risk. It describes what we built and why, including the risk analysis performed and the security/privacy control mappings. It also explains the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.
- 5G Cybersecurity white paper series: Each paper in the series includes information, guideline, and research findings for an individual technical cybersecurity- or privacy-supporting capability available in 5G systems or their supporting infrastructures. Each of the capabilities has been implemented in a testbed as part of the NCCoE project, and each white paper reflects the results of that implementation and its testing.

## Other NIST Resources Used for the Project

- *Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases* (NIST IR 8320)
- *Hardware-Enabled Security: Container Platform Security Prototype* (NIST IR 8320A)
- *Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms* (NIST IR 8320B)
- *Guide to LTE Security* (SP 800-187)

## Other 5G-Related Standards and Guideline Used for the Project

- 3rd Generation Partnership Project (3GPP) specifications, including:
  - Security architecture and procedures for 5G System (Specification #33.501)
  - System architecture for the 5G System (Specification #23.501)
  - Procedures for the 5G System (Specification #23.502)
- GSM Association (GSMA), ***Securing the 5G Era***
- Communications Security, Reliability, and Interoperability Council (CSRIC) VII, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security*

# Collaborators

We are grateful to the following collaborators for their generous contributions.

AMI: Muthukkumaran Ramalingam, Stefano Righi

AT&T: Rich Mosley*, Jitendra Patel, Bogdan Ungureanu

CableLabs: Tao Wan

Cisco: Matt Hyatt, Peter Romness*, Kori Rongey, Steve Vetter*

Dell Technologies: Dan Carroll

Intel: Steve Orrin, Leland Brown*

Keysight Technologies: Corey Piggott, Yong Zhou*

MiTAC Computing Technology Corp.: Simon Hwang, Michael Yeh*

Nokia: Gary Atkinson, Rajasekhar Bodanki, Robert Cranston, Jorge Escobar, Don McBride

Palo Alto Networks: Aarin Buskirk, Sean Morgan, Bryan Wenger

T-Mobile: Todd Gibson

* Former employee; all work for this publication was done while at that organization

## Acknowledgments

We are grateful to the following individuals for their generous contributions.

NIST: Cherilyn Pascoe, Adam Sedgewick, Kevin Stine

The MITRE Corporation: Surajit Dey, Sallie Edwards, John Kent, Blaine Mulugeta, Mary Raguso, Theresa Suloway, Charles Teague

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register. The following respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

| Collaborator | Project Build Involvement |
|---|---|
| AMI | AMI TruE |
| AT&T | 5G network design reviews<br>Security feature evaluation and implementation planning |
| CableLabs | 5G network design reviews<br>Security feature evaluation and implementation planning |
| Cisco | Cisco Secure Firewall<br>Cisco Secure Network Analytics (Stealthwatch) |
| Dell Technologies | Dell EMC PowerSwitch 3048, 4048, & 5232-ON switches<br>Dell EMC VxRail<br>Dell Networking Operating System OS10<br>Dell PowerEdge 650/750 servers |
| Intel | Intel® Security Libraries for Data Center (Intel® SecL-DC)<br>Intel Trusted Execution Technology (TXT)<br>Intel® Xeon® Gold 5218R Processor |
| Keysight Technologies | 5G LoadCore |
| MiTAC | MiTAC Aowanda<br>MiTAC Thunder SX TN76-B7102 |
| Nokia | Nokia 7705 SAR-8<br>Nokia 7750 SR-a8<br>Nokia AirScale (5G21A)<br>Nokia AWHHF<br>Nokia Cloud Mobility Manager (CMM)<br>Nokia Cloud Mobile Gateway (CMG)<br>Nokia CloudBand Applications Manager (CBAM)<br>Nokia Container Services (NCS)<br>Nokia NetAct<br>Nokia NetGuard Certificate Manager (NCM)<br>Nokia NetGuard Identity Access Manager (NIAM)<br>Nokia Network Exposure Function (NEF)<br>Nokia Network Resource Discovery (NRD)<br>Nokia Network Services Platform (NSP)<br>Nokia Policy Controller (NPC)<br>Nokia Registers<br>Nokia Shared Data Layer (SDL)<br>Nokia Telecom Application Server (TAS)<br>Nokia Zero Touch Service (ZTS) tools |
| Palo Alto Networks | Panorama<br>VM-Series N3/N4<br>VM-Series N6 Gateway |
| T-Mobile | 5G network design reviews<br>Security feature evaluation and implementation planning |

# Get Involved

## Join an NCCoE Community of Interest (COI)

A Community of Interest (COI) is a group of professionals and advisors who share business insights, technical expertise, challenges, and perspectives to guide NCCoE projects. COIs often include experts, innovators, and everyday users of cybersecurity and privacy technologies. Share your expertise and consider becoming a member of this project's COI. You can sign up for any NCCoE COIs at https://www.nccoe.nist.gov/get-involved/join-community-interest.

## Share Your Feedback on This Guide

You can view or download the preliminary draft guide at https://www.nccoe.nist.gov/5g-cybersecurity. Help the NCCoE make this guide better by sharing your thoughts with us. There will be at least one additional comment period for this volume, and the other volumes of this guide will be released for review and comment on individual schedules so that each volume is available as soon as possible.

Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more about the project and example implementation, contact the NCCoE at 5g-security@nist.gov.

## Collaborate With Us

There are a variety of opportunities for getting involved in designing, building, deploying, and documenting standards-based cybersecurity solutions at the NCCoE. The NCCoE works with members of industry to identify the most pressing cybersecurity challenges and to address technology gaps affecting multiple sectors of the economy.

**Work with us in our labs.** The NCCoE uses a formal process to solicit collaborators for its projects. For each NCCoE project, we announce a collaboration opportunity in the *Federal Register*. The Federal Register Notice (FRN) includes the project's technical requirements and details the process for organizations interested in participating. Potential collaborators can submit a letter of interest (LOI) that identifies the products, technologies and engineering expertise being offered to the NCCoE to support the project. NIST evaluates each LOI on a first-come, first-served basis and determines technical acceptability based on fit to the project's scope and satisfaction of the project's technical requirements.

Sign up for alerts from us and watch the *Federal Register* for calls for participation. Organizations that are selected to participate are required to sign a Cooperative Research and Development Agreement (CRADA). See an example CRADA.

**Become a Partner.** The National Cybersecurity Excellence Partnership (NCEP) program is an ongoing collaborative partnership between U.S. companies and the NCCoE to advance the state of cybersecurity practice. This program fosters rapid adoption and broad deployment of integrated cybersecurity tools and techniques that enhance consumer confidence in U.S. information systems. NCEP partners have pledged to provide hardware, software and expertise to support our mutual efforts to advance rapid adoption of secure technologies. In addition to contributing equipment and other products to the NCCoE's test environments, companies may designate guest researchers to work at the center, in person or remotely.

Learn more about how your organization can get involved by emailing nccoe-ncep-team@nist.gov.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

**NIST Technical Series Policies**

Copyright, Use, and Licensing Statements

NIST Technical Series Publication Identifier Syntax

**Author ORCID iDs**

Michael Bartock: 0000-0003-0875-4555

Jeffrey Cichonski: 0009-0006-1137-2549

Karen Scarfone: 0000-0001-6334-9486

Murugiah Souppaya: 0000-0002-8055-8527

**How to Cite this NIST Technical Series Publication:**

Bartock M, et al. (2025) 5G Cybersecurity (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1800-33 https://www.nccoe.nist.gov/publications/practice-guide/nist-sp-1800-33-ipd-5g-cybersecurity

**Public Comment Period**

March 18, 2025 – April 16, 2025

**Submit Comments**

5g-security@nist.gov

Or submit the web form at https://www.nccoe.nist.gov/5g-cybersecurity

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000)

Gaithersburg, MD 20899-2000

**Additional Information**

Additional information about this publication is available at https://www.nccoe.nist.gov/5g-cybersecurity, including related content, potential updates, and document history.

**All comments are subject to release under the Freedom of Information Act (FOIA).**

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE