Workshop on 5G Cybersecurity: Preparing a Secure Evolution to 5G

National Cybersecurity Center of Excellence

Workshop

October 10, 2019

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Emergency Procedures for NCCoE Visitors

Evacuation Emergencies

What is an Evacuation Emergency?

- Fires
- Explosions
- Earthquakes
- Indoor toxic material releases
- Indoor radiological and biological accidents
- Workplace violence

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest exit (**Red Signs – Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction
- Once outside the building, swiftly walk toward the designated meeting area near the posted sign stating "Evacuation Meeting Area" (**Yellow Sign – Lower Right Map**)

Shelter-In-Place (SIP) Emergencies

What is a Shelter-In-Place Emergency?

- Severe weather (hurricanes, tornadoes, etc.)
- chemical, biological, or radiological contaminants released into the environment

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest SIP hallway or room (**Yellow Signs – Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction

Agenda

8:30 - 9:00	***Check-in***
9:00 - 9:15	NIST and NCCoE Overview
9:15 - 9:45	Overview of the NIST 5G Cybersecurity Initiative
Invited Industry Presentations	
9:45 - 10:00	AT&T
10:00 - 10:15	T-Mobile
10:15 - 10:30	Sprint
10:30 - 10:45	Ericsson
10:45 - 11:00	Nokia
11:00 - 11:15	Cisco
11:15 - 11:30	***Break***
11:30 - 11:45	Intel
11:45 - 12:00	Red Hat
12:00 - 12:15	CableLabs
12:15 - 13:00	Industry Panel Q&A
13:00 - 13:15	Wrap-Up

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

National Institute of Standards and Technology

National Institute of Standards and Technology

NIST is a bureau under the Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST runs a number of laboratories to assist in its mission.

Communications Technology Laboratory	Engineering Laboratory	Information Technology Laboratory	Material Measurement Laboratory	Physical Measurement Laboratory

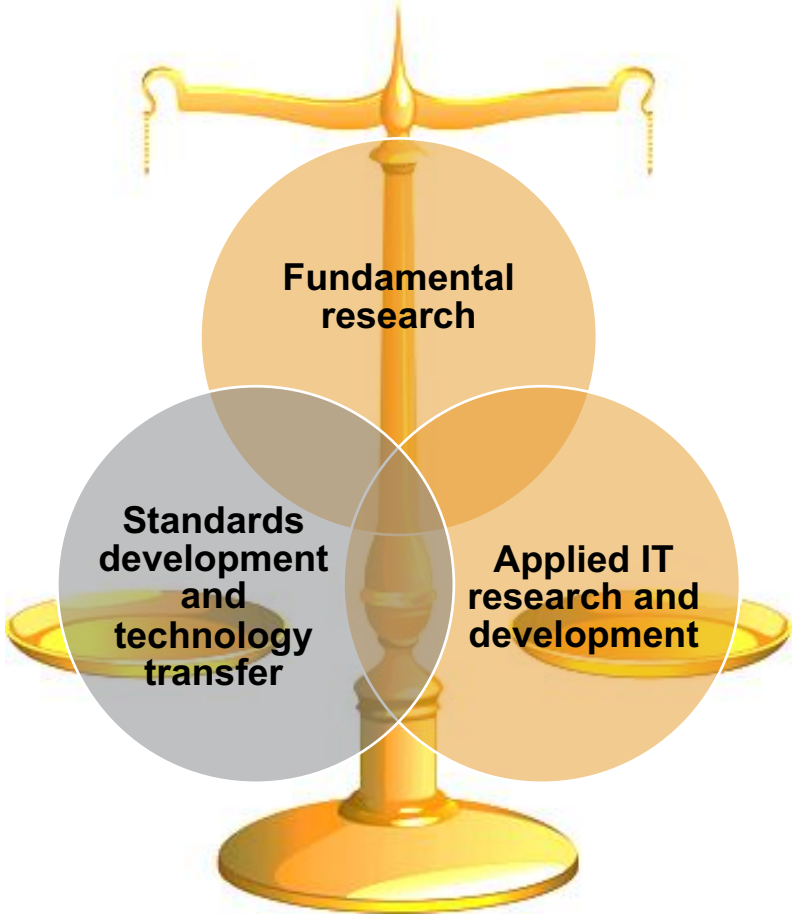
NIST Information Technology Laboratory – itl.nist.gov

Cultivating trust in IT and metrology through measurements, standards, and tests

Cybersecurity Program

Standards and Guidelines Development – csrc.nist.gov

- Cryptographic Development – AES, SHA-3, PQC, etc.
- Cryptographic Validation – FIPS 140-2
- Risk Management Framework – Cybersecurity Framework, FISMA, SP 800-53, SP 800-171, etc.
- Technology Guidelines – Virtualization, Containers, Security Automation, etc.
- Privacy Framework
- Identity Management



National Cybersecurity Center of Excellence (NCCoE) – nccoe.nist.gov

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

Collaboration with Industry, Federal/State/Local Governments, and Academia

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Introduction to NCCoE

NCCoE Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

NCCoE Tenets

Standards-based
Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable
Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available
Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable
Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent
Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

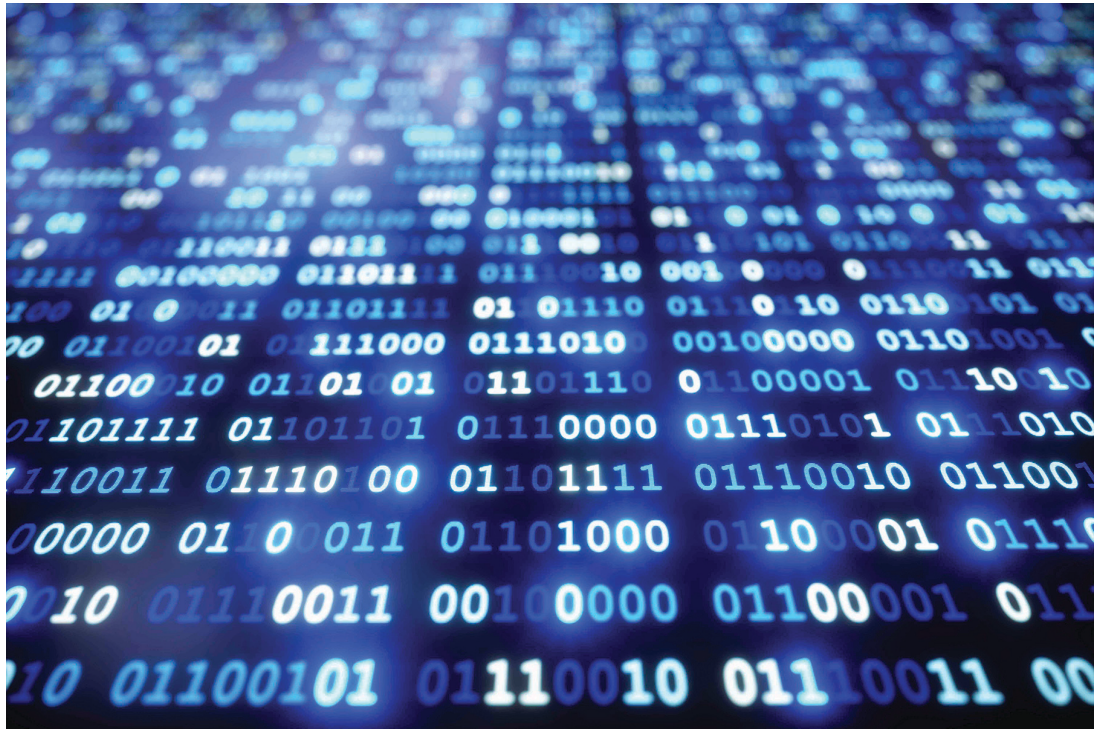
- Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

Sector-Based Projects



- Commerce/Retail (SP 1800-17)
- Energy (SP 1800-2 & SP 1800-7)
- Financial Services (SP 1800-5 & SP 1800-9 & SP 1800-18)
- Healthcare (SP 1800-1 & SP 1800-8)
- Hospitality
- Manufacturing
- Public Safety/First Responder (SP 1800-13)
- Transportation

Cross-Sector Projects

- Attribute Based Access Control (SP 1800-3)
- Data Integrity (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Secured Email (SP 1800-6)
- Mitigating IoT-Based DDoS (SP 1800-15)
- Mobile Device Security (SP 1800-4 & SP 1800-21)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Management (SP 1800-16)
- Trusted Geolocation in the Cloud (SP 1800-19)

Purpose and Objective of the Workshop

Purpose

- Explore the ***practical and implementable cybersecurity capabilities*** delivered by 5G systems
- Identify existing ***industry recommended practices*** for securing the supporting infrastructure and technologies
- Understand potential ***opportunities and challenge areas*** affecting this evolution to 5G
- Present ***notional topics*** to kick-off the discussion of 5G security journey
- Solicit ***feedback from the community***

Objective

- Inform the development of potential NCCoE demonstration projects to leverage ***5G cybersecurity capabilities*** and supporting technologies to protect the cellular communication network in addition to ***secure the core 5G underlying infrastructure and services***

Attendees

199 registrants

Registrants' organizations breakdown:

- Government – Federal, State, Local, Academia
- Private Industry – Telecommunication, Information Technology, and Financial Services
- Consulting Companies
- Non-Profits/Not-for-Profits
- Welcome to the Press!

Workshop on 5G Cybersecurity: Preparing a Secure Evolution to 5G

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Today's Topics

- New Security Features
- 5G Notional Architecture
- Supporting Infrastructure and Security Protocols
- 5G Use Cases
- Potential Topic Ideas
- Objectives and Goals

5G Cybersecurity at The NCCoE

Enhanced Security Capabilities

Demonstrate increased cybersecurity protections in 5G networks from the addition of standards based features

Modern Supporting Technologies

Increased use of modern information technologies Supporting the 5G System to allow for the addition of modern cybersecurity best practices

Practical Approach

As 5G technologies are still being specified and developed it's important to effectively scope and prioritize this effort

New Security Features

- User Plane Traffic Integrity
- Subscriber Identifier Privacy
- Security Edge Protection Proxy
- Increased Home Control
- Unified Authentication Framework
- CU / DU Separation

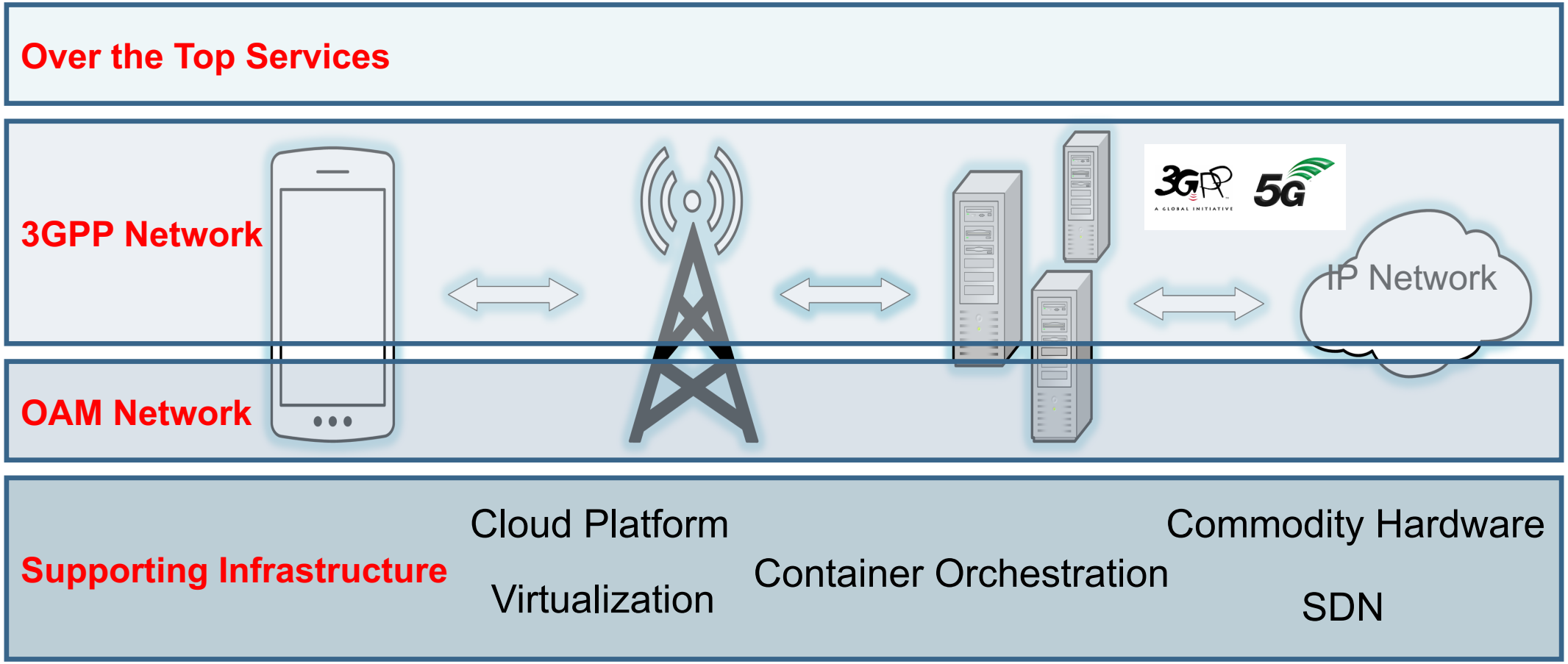
So What's the Scope

- 5G networks are comprised of many components utilizing different modern information technologies

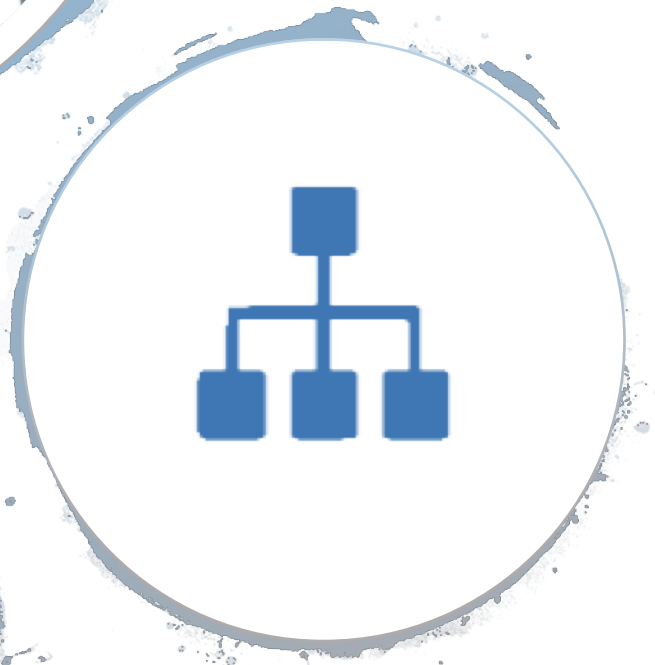
- 3GPP Network Functions are ONLY one piece of the evolution to 5G deployments

- Cybersecurity best practices used for the various components of the technology stack

Notional Architecture



Supporting Infrastructure and Security Protocols



- Cloud computing platforms
  - Virtualization
  - Containerization
  - Orchestration
- Internet security protocols
  - IPSec
  - TLS
  - JOSE, etc.

Driven By Use Cases

Enhanced Capabilities on Commercial Mobile Networks

Non Public Networks i.e. the use of 5G in industrial control system environments

Edge Computing

The use of 5G to support enterprise mission and business objectives

5G Cybersecurity Topic Ideas

- **Secure Cloud Deployment –** Secure deployment of core and ran network services on 'cloud like' infrastructure to include; hardware roots of trust, network function virtualization best practices such as ETSI NFV Sec (eg ETSI GS NFV-SEC 012)
- **Edge Computing –** Security of edge computing deployments enabled by 5G networks
- **Secure Slice –** The use of network slicing to provide a higher level of assurance to customers with unique security requirements. This could focus on enabling standards-based security features as well as operational/deployment best practices
- **Visibility API –** Applied research related to the UE RAN connection to include the visibility API specified in R15 3GPP 33.501 to allow applications to make informed decisions based on the security characteristics of their current RF connection
- **Disable 2G Radio Access Technologies on UE –** Mitigating threats posed by legacy cellular network technologies with standards-based capabilities
- **Virtual Radio Access Network –** Virtualization is also becoming common in the RAN of 5G networks; a pool of virtual resources will be able to share signaling among cells.

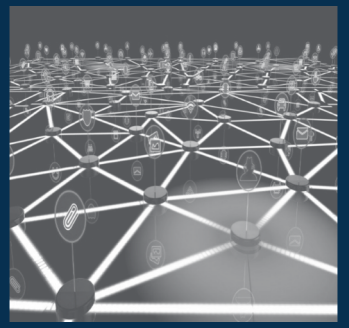
Objective and Goals

Roadmap

Cybersecurity topics of interest shape the NCCoE's 5G Cybersecurity Roadmap.

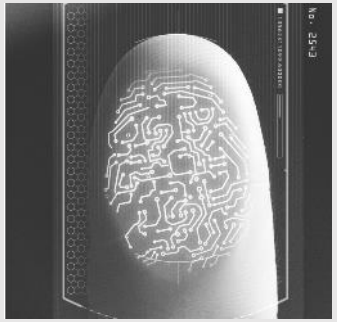
Priorities

Cybersecurity topics are prioritized in a rational way that reflect 5G technology availability.



Projects

NCCoE project descriptions, builds and practice guides are developed to address topic requirements.



Influence

Real world solutions demonstrating robust copiabilities surrounding 5G networks.

Wrap Up: We Value Your Feedback

Do you:

- Have additional comments/feedback regarding our project?
- Have an idea that you think the NCCoE should pursue?
- Know of an event where NCCoE should present?

Please engage with us: 5G-Security@nist.gov

http://www.nccoe.nist.gov

301-975-0200

nccoe@nist.gov