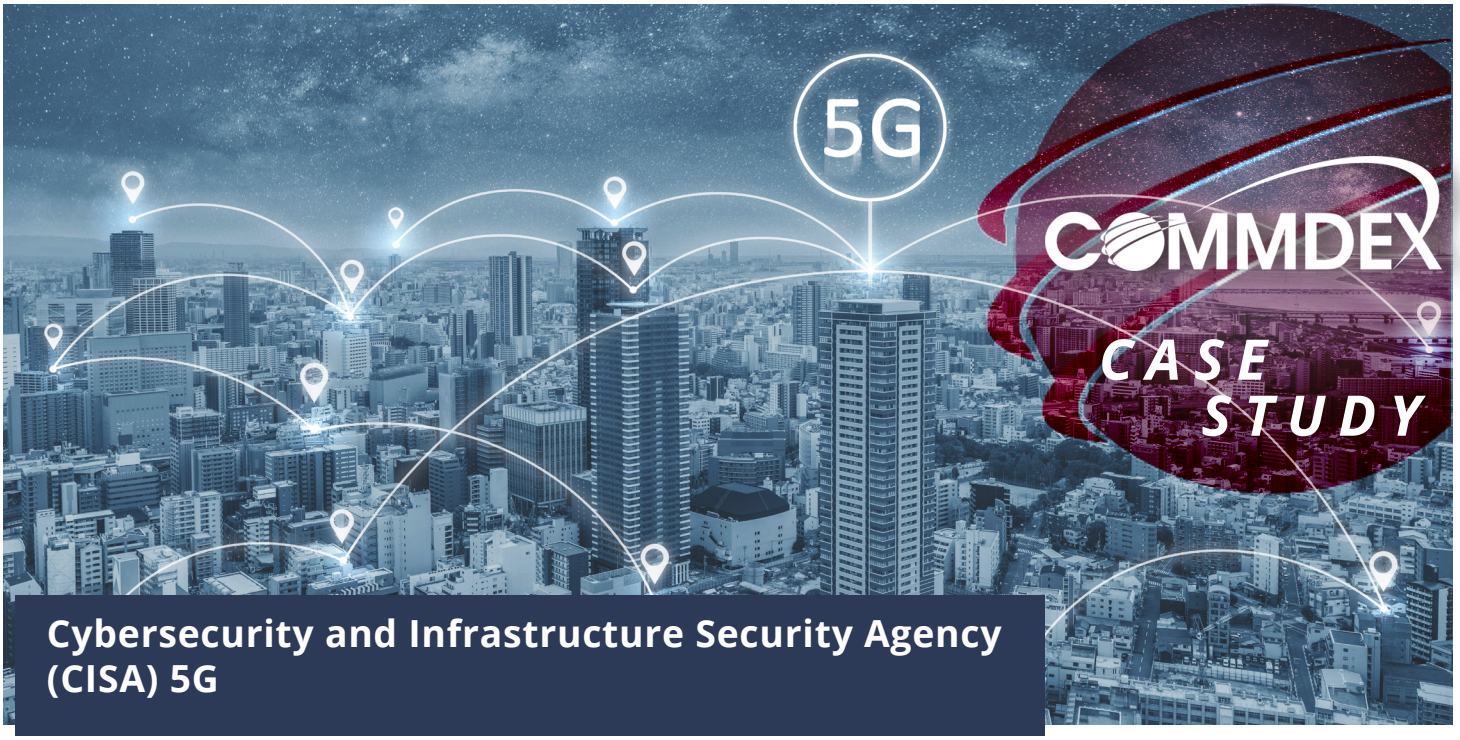


Cybersecurity and Infrastructure Security Agency (CISA) 5G

Location:
Washington D.C.

Business Needs:
A comprehensive lab testing environment for 5G architecture and security capabilities

Customer Challenge

CISA had a need to produce a security and privacy architecture specification that aligns with commercial 5G architectures and adheres to 3GPP standards. CISA's goal is to develop security capabilities that leverage 5G virtual functions/network slicing and define methods/approaches to achieve this. To develop this specification, it needed to develop and evaluate various end-to-end security controls for 5G devices, 5G Radio Access Network, core, and transport network architecture in a contractor-operated Laboratory environment.

Customer Profile

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. It connects the stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.

CISA acts as the quarterback for the federal cybersecurity team, protecting and defending the home front—our federal civilian government networks—in close partnership with the Office of Management and Budget, which is responsible for federal cyber security overall. CISA also coordinates the execution of our national cyber defense, leads asset response for significant cyber incidents, and ensures that timely and actionable information is shared across federal and non-federal, and private sector partners.

Commdex Solution

Commdex is supporting the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) as part of the Security and Resiliency of Mobile Network Infrastructure (SRMNI) project. The SRMNI project is in direct response to the US National Security Strategy and a validated requirement from the DHS CISA. The goals of this project cover a range of security assessments of 5G systems, including:

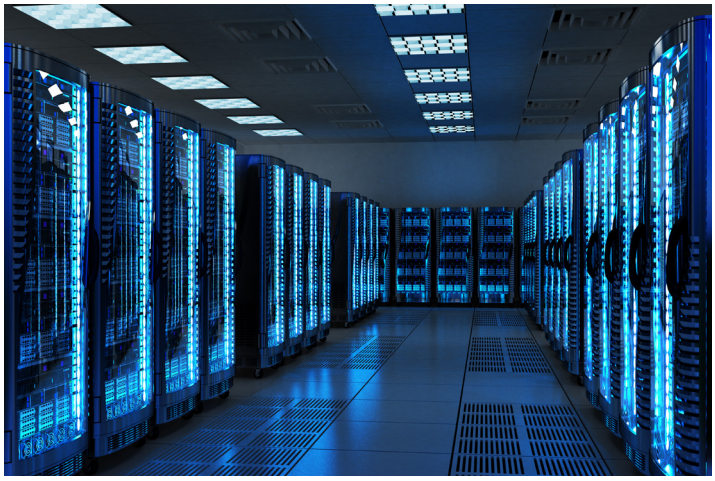
Goal 1 - Unified Family of 5G Security Techniques
Goal 2 – Security Architecture for Government Using Network Slicing
Goal 3 – End-to-End Security from the Mobile Device to the Core

Commdex has partnered with Nokia to provide a lab-as-a-service approach to delivering a variety of testing scenarios and use cases that provide actionable findings that support these goals.

2400 Herodian Way, Suite 360
Smyrna, GA 30080

sales@commdex.com
www.commdex.com

Commdex Roles



Research and Design: Commdex designed and documented the Fifth Generation (5G) Network Security solution. The design document described an end-to-end network security strategy and architecture document that encompassed research, design, and architecture of the network security solution.

The Commdex-provided design document outlined the research, development, testing, and piloting strategy for end-to-end security controls for a 5G device, RAN, core, and transport network architecture aligned with the network architecture that national Wireless Service Providers will be implementing in their networks. This design document demonstrated how properly developed and implemented security controls, processes, and procedures will increase the security and resiliency of 5G infrastructure to reduce the risks to Government services, devices, and data utilizing LTE as the anchor for control and signaling and 5G networks.

The design document addressed what types of attacks can occur at these various vulnerable areas of the network architecture and how the developed security controls will mitigate these risks and vulnerabilities. The document also detailed how the security controls will meet DHS and contractor agreed-to functional and performance requirements for end-to-end security with mutually agreed-to Key Performance Indicators (KPIs).

Finally, the design document addressed how to ensure priority services for emergency communications during congestion events on 5G infrastructure. The document describes approaches to identifying a TDoS, DDoS/Massive IoT attack from congestion during a NS/EP event and recommends security controls that prevent degradation or impairment of priority services for NS/EP communications.

Integration and Deployment: Based on the design document developed as part of the Research and Design phase, Commdex configured a 5G lab that was equipped and configured to perform testing to validate the aspects of the architecture document. We developed and delivered an installation and checkout plan to verify system operation and performance, meeting the Target Capabilities Definition Document. We then developed an Integration and Deployment strategy along with a plan document that described the methodology of how developed security controls met functional and performance requirements.

Test and Evaluation: As part of testing, Commdex provided a Testing and Evaluation (T&E) document including high-level test strategy, methodology, test tools (e.g., packet monitoring, simulation tools for congestion or DDoS attacks), test cases for both security functionality and performance, test pass/fail criteria per KPIs, and test artifacts (e.g., operational security measurements, security control operational settings/configuration, call/data session traces). Commdex then executed the test cases with DHS witnesses at the 5G lab facility. This was performed using actual production network elements and contractor-recommended security controls per major US carrier representative architecture.

Test strategy and test cases verified function and performance of:

- Security control identification and mitigation of various types of DDoS, or massive attacks at the edge of the network
- Direct physical attack on Remote Radio Units (RRU)
- Man-in-the-middle or spoofing attacks to infiltrate, exfiltrate, or maliciously alter signaling or traffic on the network on a per-user and per slice basis
- Malware attacks
- Attacking a weaker network slice to get access to a higher-value target network slice
- Continuity of security and priority of federated network slice across dissimilar network segments
- Detection of anomalous traffic and signaling patterns while maintaining priority services KPIs such as WPS, GETS, and those used by FirstNet and commercial priority service providers
- Edge computing security control capability to detect and “wall off” or load balance certain attacks at the edge of the network.
- Network to network interface security control to detect and stop or mitigate attacks from other service providers, Internet, or cloud computing providers