U.S. NATIONAL SECURITY AGREEMENT AND U.S. CARRIER COMPLIANCE STANDARDS

1. General

Supplier activities must comply with the U.S. National Security Agreement (NSA), which Nokia signed with the U.S. Government to address national security concerns. To ensure compliance, relevant NSA obligations must be contractually passed down to suppliers s

Capitalized terms in herein not defined in the Agreement shall have the meanings provided in section 2 Definitions below.

In case of a conflict between the terms herein and any other Agreement provision, these terms will prevail.

A breach of the terms herein by Supplier will be considered a material breach of the Agreement.

2. Definitions

The following definitions apply the terms herein.

Authorized Personnel – means any person or persons who have met the requirements for access to, and handling of, NSA Protected Information, or access to U.S. Communications Infrastructure, as may be applicable and, when required, have been placed in the applicable ACL (Access Control List maintained in Nokia's Compliance, Auditing and Privacy System (CAPS)) Group unless otherwise approved by the NSA Security Officer.

CALEA Product – means a Product that has the capabilities, functionalities, and features that are developed and implemented for the purpose of complying with the U.S. Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, et seq., and any successor statute that imposes substantially the same obligations ("CALEA").

Class A Product – refers to former Alcatel-Lucent Products, 5ESS (including DNU-S, EXM, SM2K), 5ESS Wireless MSC (9253 OMC-RAN, 9254 OMC-RAN Compact, 9256 OMP, 9271 EVDO-RNC, 9281 PS, 9281 PSC, 9290 MM, 9290 MMC), GTD-5, 4ESS products and any key modules or intellectual property uniquely associated with them, or as updated from time to time.

Contractors – Individuals who are not employees of Nokia but provide temporary services (such as clerical, administrative, management, professional, or technical) to Nokia on a contract basis through a third party. They are generally compensated on a time and materials basis. These contractors offer individual-based staff augmentation or project-based work and are employees of a third-party supplier. Contractors with access to Nokia IT systems containing U.S. Customer data, U.S. Communications Infrastructure, U.S. Government Customer information, or NSA Protected Information must be registered as contractors with Nokia and apply to be Authorized Personnel via the Compliance, Auditing, and Privacy System (CAPS).

D1, E1 and E2 Countries – means the countries identified in the current Supplement No. 1 to Part 740 of the U.S. Export Administration Regulations issued by the Bureau of Industry and Security. Note: In December 2020, the USG amended the Export Administration Regulation to specify Hong Kong will be treated the same as China.

Design Information – Design Information refers to documentation created during product development that describes the implementation and functioning of hardware or software. Design Information includes, but is not limited to, hardware architecture specifications, software architecture specifications, hardware implementation specifications, schematics, circuit descriptions, software interface specifications, and software design specifications.

Designated Contact – means the contact details specified in section 9 below, serving as the primary point of contact for the Supplier regarding all NSA-related matters, including contacting Nokia's NSA Security Officer.

NSA Security Officer – means the Nokia employee appointed as such pursuant to the requirements of the NSA with primary responsibility for Nokia's compliance with the NSA.

Outsourced Workers – Employees of a third party that supplies services to Nokia under specific projects with a pre-defined scope and milestone deliverables. These workers perform projects that are not part of Nokia's core business and are not executed by Nokia employees. Outsourced Workers with access to Nokia IT systems containing U.S. Customer data, U.S. Communications Infrastructure, U.S. Government Customer information, or NSA Protected Information must be registered as contractors with Nokia and apply to be Authorized Personnel via the Compliance, Auditing, and Privacy System (CAPS).

Proprietary Customer Information - means information of the types itemized below about a Nokia customer's network, services, or operations that customers typically consider proprietary. This information may be either provided by the customer to Nokia or derived by Nokia from its customer support operations. In the context of Class A Products, Proprietary Customer Information is the following: information disclosing specific network equipment in locations and its interconnection in networks; detailed office cabling information (e.g., information that provides a comprehensive view of the cabling interconnect assignments within the office such as cabling schematics/wiring lists, etc.); information about how individual end user calls are routed in customer networks (including network address information such as trunk ids, IP addresses of internal customer networks, machine translations etc.); equipment logs and other routinely generated information from equipment deployed in customer networks and customer-provided switch databases; data files associated with Class A equipment configurations (e.g. ECD's – Equipment Configuration Data); and such other information that Nokia from time to time informs the Supplier should be treated as Proprietary Customer Information.

SDHLR Product – means 1440 Unified Subscriber Data Server, 8650 SDM Expert, 8650 Subscriber Data Manager, Virtualized Subscriber Data Manager (vSDM) or as updated from time to time.

Sensitive Information – means (i) Sensitive Product Information relating to a Class A Product; (ii) Proprietary Customer Information relating to a Class A Product; (iii) Service Provider End User Information related to a Class A Product or SDHLR Product; and (iv) U.S. Government Customer Information, as those terms are defined below and such other categories of data related to Nokia's NSA as may be identified in writing from time to time.

Sensitive Product Information – means information unique to a Class A Product including, but not limited to: source code, Design Information (Software and Hardware), build environments (base source code, general libraries, make files, software tools and linkers, compiled/executable object and/or delivered package, and checksum/hashsum information and programs), software change control system.

Service Provider – means an entity that carries U.S. domestic communications traffic for end user customers using products or services provided by Nokia.

Service Provider End User Information – means any customer identifying information for any customer of a Service Provider including the end user customer name, address, phone number, e-mail or IP address, or any other information that is customarily used to identify a particular end user customer.

Supplier - The party supplying products and services to Nokia under the Agreement (covering both Contractors and Outsourced Workers).

U.S. Communications Infrastructure – means any part of a communications network deployed in the U.S. by any Nokia customer (U.S. or non-U.S. service provider or private business) or deployed by the U.S. Government anywhere in the world.

U.S. Government Customer Information– means, unless made public by the US Government, any identifying information (such as name of agency or person, address, telephone number, email address, IP address, or any other information) that can be used to identify a US Government customer or a US Government end user, or records or information in any form (including, but not limited to, written, electronic, stored or transmitted) pertaining to the needs of and purchases by the U.S. Government, including but not limited to research, products, services, or software needs, whether purchased directly from Nokia, a Nokia affiliate or through a reseller.

U.S. Government Sensitive Information or U.S. Government Sensitive Technology – means U.S. Government information or technology, other than classified information or classified technology, that is designated in writing by an authorized official as "Sensitive Information," "Official Use Only," "Limited Official Use Only," "Law Enforcement Sensitive," "Sensitive Security Information," "Not For Distribution to Foreigners," "NOFORN," or other similarly designated categories.

3. Access to and Handling of NSA Protected Information

3.1. Supplier's provision of products and services, pursuant to the Agreement, may involve access to Sensitive Information or Service Provider End User Information (SPEUI) ("NSA Protected Information"). U.S. Government Customer Information has a dedicated section 4.

3.2. The Supplier shall access NSA Protected Information only from locations approved by Nokia's Customers and will contact the Designated Contact to determine the specific type of NSA Protected Information to be accessed and to identify the associated Nokia Customers. Final approval will be provided by Nokia's NSA Security Officer.

3.3 Control and Access of NSA Protected Information

Supplier must ensure the protection of NSA Protected Information, whether it resides on Supplier's systems or is accessed on Nokia's systems.

Storing or Accessing NSA Protected Information on Supplier's Systems: Supplier must implement and maintain robust security measures, including but not limited to:

- Encryption of data at rest and in transit.
- Multi-factor authentication for access.
- Regular security audits and vulnerability assessments.
- Incident response procedures.
- Supplier shall maintain an auditable list of all personnel (including subcontractors) approved for access to NSA Protected Information on its systems.

Storing or Accessing NSA Protected Information on Nokia's Systems: Supplier personnel must adhere to the following protocols:

- Use only authorized and secure methods for system access.
- Implement strict access controls, including the principle of least privilege.
- Maintain detailed access logs and regularly review them for unauthorized activity.
- Supplier personnel must complete appropriate Nokia training and be placed on relevant Nokia ACLs for access to Nokia systems and U.S. Communications Infrastructure.
- Nokia will maintain records of training and approval for Supplier personnel accessing its internal network. Supplier shall maintain an auditable list of its personnel (including subcontractors) approved for accessing NSA Protected Information on Nokia systems.

Supplier is required to provide the auditable list of approved personnel to Nokia's NSA Security Officer upon written request.

3.4. Access to and handling of NSA Protected Information is limited to Authorized Personnel, who must ensure it is not further disseminated except to other Authorized Personnel.

3.5. The Supplier must verify that individuals are Authorized Personnel before disclosing NSA Protected Information and can obtain assistance through the Designated Contact for verification.

The Supplier shall only access NSA Protected Information that is strictly required for its services. If any NSA Protected Information is received that is not required or is accessed without authorization, the Supplier must immediately notify the NSA Security Officer and handle it according to their instructions.

3.6. Access to SPEUI is limited to Authorized Personnel and the minimum necessary information required for specific services. Such access must also comply with Service Provider remote offshore access requirements, including those for approved offshore countries.

3.7. For access to Service Provider End User Information related to Class A or SDHLR Products, individuals must apply for specific access permission in the -Nokia's ACL group as described in section 6. Only Authorized Personnel may access the SPEUI information.

3.8. SPEUI may only be retained for the minimum time required to complete the service. Once no longer needed, it must be destroyed (with certification to Nokia upon request) or returned to Nokia. Archival retention of SPEUI is strictly prohibited.

3.9. SPEUI associated with SDHLR products must remain in the U.S. at all times.

4. U.S. Government Customer Information

4.1. Access Restrictions: Access to U.S. Government Customer Information is limited to those who need it for specific services and must be restricted to the minimum necessary information. Persons from D1, E1, and E2 Countries (as defined in section 1) cannot be Authorized Personnel.

4.2 All personnel requiring access to USG Customer Information, whether stored on Supplier or Nokia systems, must meet the following criteria to be considered Authorized Personnel:

Training Completion:

- Storing or Accessing USG Customer Information on Supplier's Systems: Personnel must certify they have read and understood Nokia-provided training, delivered either through live sessions or electronic materials. The Supplier is responsible for providing a certification for each trained individual.
- Storing or Accessing USG Customer Information on Nokia's Systems: Personnel must complete the applicable Nokia training and be placed on relevant Nokia ACLs for access to USG Customer Information.

Access Control and Certification:

- Storing or Accessing USG Customer Information on Supplier Systems: The Supplier must maintain an ACL of all personnel certified as trained in handling USG Customer Information.
- Storing or Accessing USG Customer Information on Nokia Systems: Personnel must obtain specific access permission by applying for authorization within the appropriate ACL group, as detailed in the ACL and Background Screening under section 6.

Only individuals who fulfill all training and certification requirements and receive explicit approval will be granted access to USG Customer Information.

5. Specific Requirements for Access to U.S Communications Infrastructure

5.1 Access to U.S. Communications Infrastructure and customer networks containing Service Provider End User Information (SPEUI) is strictly controlled.

5.2 General Requirements for Access to U.S. Communications Infrastructure

If Supplier services require access to Nokia's customers' U.S. Communications Infrastructure, the following apply:

- Access must comply with the ACL and Background Screening under section 6.
- Remote access must be secure and encrypted, unless explicitly waived by Nokia in writing. Supplier remote access solutions will undergo case-by-case review to ensure adequate controls.
- Remote access from outside the U.S. requires written approval from the NSA Security Officer.

- Supplier must adhere to the applicable customer's requirements as directed by Nokia's Customer.

5.3 Additional Requirements for Access to Customer Networks Containing SPEUI

Access to customer networks containing SPEUI depends on whether the information resides on Supplier or Nokia systems.

Supplier Systems

- Personnel requiring access must certify they have read and understood Nokia-provided training (live or electronic). The Supplier must provide a certification or attestation for each trained individual.
- The Supplier must maintain an ACL ("Supplier ACL") for personnel certified in handling SPEUI.
- Only certified and approved personnel are considered Authorized Personnel for accessing systems containing SPEUI.

Nokia Systems

- Personnel requiring access must complete the applicable Nokia training and obtain specific access permission by applying for authorization within the appropriate ACL group, as described in section 6.

6. Access Control List (ACL) and Background Screening

6.1. If Supplier is hosting or accessing Nokia Sensitive information on Supplier systems:

Supplier shall maintain an ACL identifying Authorized Personnel with access to Nokia Sensitive Information and/or U.S. Communications Infrastructure via Supplier's systems only. Only Authorized Personnel on the Supplier's ACL shall be granted authorizations specific access permissions for different groups based on the nature of the access required. Such Supplier personnel may be in multiple Supplier ACL groups as designated by the Supplier.

Supplier personnel, including their supervisors, must undergo background screening to be granted access to Supplier's ACL. This screening shall either adhere to Nokia's requirements (and comply with applicable laws) or, if privacy regulations preclude Nokia's direct screening, the Supplier must provide formal attestation of their own completed background screening. To maintain ACL access, an initial screening and subsequent re-screens, conducted randomly every five (5) years, are required.

Upon NSA Security Officers written request, Supplier shall make available Supplier's ACL. ACL Information will include, 1) name of personnel, 2) location of personnel, 3) originating IP address of where the access took place from, 4) date and time stamps of access to either Nokia Sensitive Information on Supplier systems or Nokia systems deployed within the U.S. Communications Infrastructure.

Nokia reserves the right to request Supplier to deny or remove persons from Supplier ACL groups for compliance obligations under its NSA or for security reasons. Removed personnel must be immediately denied access to all Sensitive Information and means of access (e.g. assigned computers, backups, etc.) to the U.S Communications Infrastructure.

6.2. If Nokia Sensitive Information is being stored or accessed on Nokia systems:

Nokia shall maintain an ACL identifying Authorized Personnel with access to Nokia Sensitive Information and/or U.S. Communications Infrastructure via Nokia systems only. Only Personnel on the ACL shall be granted authorizations specific access permissions for different groups based on the nature of the access required. Such Supplier personnel may be in multiple ACL groups.

Nokia reserves the right to deny or remove persons from ACL groups for compliance obligations under its NSA or for security reasons. Removed personnel must be immediately denied access to all Sensitive Information and means of access to systems such as assigned computers, backups, etc.

All candidates must successfully complete all mandatory training via Nokia's online training portal. Proof of completion of all mandatory training is required in the rare event courses are completed offline. Proof of completing mandatory training courses specified by Nokia for the ACL group. Nokia may require periodic re-training to remain on the ACL.

6.3 Other restrictions may include geography, U.S. citizenship, or previous employment at Nokia or its subsidiaries.

6.4 Supplier Authorized Personnel using Nokia's remote access systems for virtual network access to the U.S. Communications Infrastructure will be listed in Nokia's directory as contractors and assigned an administrative approver on the ACL.

6.5 Supplier must ensure personnel who are on Nokia's ACL remain current including but not limited to, a) applying for authorization in a timely fashion, b) informing Nokia to remove promptly any personnel who no longer require authorization (e.g., due to a change of the Supplier Personnel's job function or assignment, etc.).

6.6 Background screening includes, but is not limited to the following: 1) identity verification, 2) criminal convictions, to the extent permitted by applicable laws, for the past seven years, if feasible; 3) employment history, including any history of disciplinary action, subject to data privacy requirements and applicable laws for the past five years, 4) education, 5) prohibited parties screening, 6) Global Sanctions List, 7) drug testing to the extent permitted by applicable law, and 10 Panel Drug screening for personnel located in the U.S., 8) military history verification, 9) National Sex Offender Registry (U.S. only); and 10) solely if the job function involves operation of a motor vehicle, driving records; all of the aforementioned in accordance with applicable law, and covering the time periods required under Nokia's background screening policies.

6.7. The information requested and provided in response to the questions on the application forms and background screening results shall be provided to Nokia. Supplier shall retain a copy of all information provided to Nokia as well as any supporting documentation received from the background screening not submitted to Nokia with the application. Such information and documentation shall be made available for inspection by Nokia upon Nokia's written request. Nokia will maintain records of training courses provided by Nokia to Supplier personnel.

Nokia will accept "results only" submissions from Supplier if providing full reports is not permissible by law or Supplier's corporate policy does not permit sharing of background screening documentation.

6.8. Supplier must provide no more than 48-hour notice to Nokia (a) upon becoming aware that any Authorized Personnel has committed a criminal offense, violated Supplier or Nokia compliance policies or submitted false information in connection with the background screening process or (b) if the Supplier personnel designated as Authorized Personnel ceases to be employed by Supplier. In the case of (b), if such Supplier personnel was terminated for cause, the notice shall so indicate, subject to applicable law.

7. Physical and Systems Security, Personnel Matters; Subcontracting and Location Restrictions

7.1. If Supplier uses third-party IT service providers that access or store information outside the U.S., it may do so provided such vendors are not located in D1, E1, or E2 countries, except for NSA Protected Information and other Service Provider information specifically designated as not being stored outside the U.S. For USG Customers, D1, E1, and E2 countries apply. For Nokia Service Providers, D1, E1, and E2 countries may not apply, but their Service Provider requirements will apply.

7.2. Subcontracting or performing services that involve NSA Protected Information or U.S. Communications Infrastructure requires prior written consent from Nokia's NSA Security Officer.. Approved subcontractors must comply with all these terms. Services performed outside the U.S. may be subject to additional restrictions and requirements.

8. Incident Reporting and Support Requirements

8.1. Supplier agrees to annually certify with the Designated Contact that it has policies and procedures in place to comply with these terms s and has performed accordingly.

8.2. Supplier agrees to notify the NSA Security Officer within twenty-four (24) hours upon discovery of any breach of the requirements of these termss or of any incident (including potential data breaches) relating to the NSA Protected Information or the systems or facilities used with respect thereto, including notifying Nokia of any incidents of actual, attempted or suspected access by unauthorized persons. Supplier agrees, at no additional cost to Nokia, to assist and provide all reasonable and necessary cooperation to Nokia in connection with any investigation of such incidents, and to take all remedial steps that may reasonably be required with respect to Supplier's personnel and scope of work. Supplier shall provide Nokia's NSA Security Officer access to all relevant information relating to NSA Protected Information or Class A Products, CALEA Products, and SDHLR Products, which Nokia may share with the U.S. Government or others monitoring Nokia's NSA compliance if necessary.

8.3. Supplier must support Nokia's NSA compliance audits, including participation in Nokia's audit cycle (third-party and internal). This support entails providing qualified personnel for interviews, meetings, records, and auditor testing. Nokia will cover its own audit costs, and Supplier will not be compensated for its participation.

8.4. For the avoidance of doubt, information concerning matters addressed in these terms (including, but not limited to, audit results and any information Supplier is required to report hereunder) or concerning security incidents related to the services (including, but not limited to, incidents that potentially affect the security of any Nokia's or Service Provider networks) shall be considered Nokia's and/or Service Providers Information as defined in the Agreement.

9.0 Designated Contact

Is a person identified to Supplier as a contact for NSA-related matters, as may be updated from time to time by written notice from Nokia to Supplier. If no specific contact is designated, the NSA Security Officer will be the Designated Contact and can be reached at the following email address:

nsa_compliance_office@nokia.com