

Terms of Reference for Short-Term Expert(s) Providing Capacity Building for the Prevention of Caller ID Spoofing and Telephone Scams in the Dominican Republic

Organisation: HAUS Finnish Institute of Public Management Ltd

Project: Finnish Digital and Green Transition (FDGT)

Host Organisation: The National Cybersecurity Center of the Dominican Republic (CNCS)

1. Purpose of the Document

This Terms of Reference defines the requirements for procuring a Short-Term Expert (STE), or a team of up to two complementary STEs, to support the National Cybersecurity Center of the Dominican Republic (CNCS) in strengthening national capacity to prevent caller ID spoofing and related telephone scams, as further described below.

The assignment is implemented under the Finnish Digital and Green Transition (FDGT) project, which deploys Finnish expertise through targeted secondments to support human-centred digital transformation in partner countries.

The focus of this assignment is on assessing and strengthening the Dominican Republic's capacity to prevent caller ID spoofing and related telephone scams. The assignment will identify key technical, regulatory and operational gaps, develop practical recommendations, and strengthen national capacity through knowledge transfer and stakeholder cooperation.

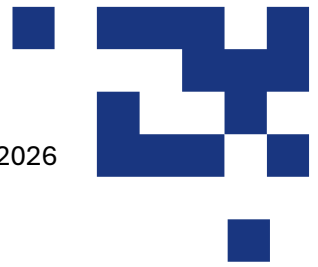
The Client (HAUS Finnish Institute of Public Management Ltd) reserves all rights to amend, modify, edit, update and withdraw this document and the information contained herein.

2. Background

Finnish Digital and Green Transition Project (FDGT)

The goal of the FDGT project (2025-2027) is to promote human-centred digital development in Africa, Asia and Latin America in partnership with Finland. The FDGT project focuses on:

- Offering short-term secondments whereby experts from Finland are sent to work in public organisations in Africa, Asia and Latin America for up to 6 months. Secondment is a means to support Digital and Green Transition in these regions by offering technical assistance based on Finnish good practices in digitalisation, while having a unique chance to forge partnerships with local stakeholders.



- Supporting the introduction of Finnish expertise and digital concepts to various international initiatives, including Team Europe Initiatives under the EU Global Gateway strategy to respond to the needs in Africa, Asia, Latin America and the Caribbean.
- Providing high-quality and timely expert services for the coordination of the EU and its Member States work in promoting human-centred digital development in the Digital for Development (D4D) Hub in Brussels.

FDGT is a **development cooperation project** funded by the **Finnish Ministry of Foreign Affairs** and implemented by **HAUS**.

3. Context and Host Organisation

The STE(s) will be seconded to the **National Cybersecurity Center of the Dominican Republic (CNCS)**.

Identified Need and Opportunity

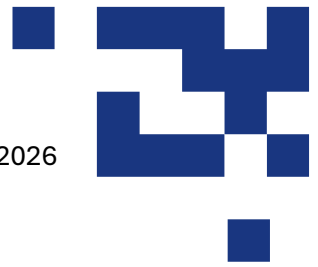
The Dominican Republic is facing a growing challenge from telephone scams involving caller ID spoofing and other forms of impersonation. These scams contribute to financial losses and cybercrime and undermine public trust in telecommunications services. While the country has established cybersecurity capabilities, capacities for caller identification and authentication, spoofing detection, fraudulent traffic analysis and call traceability remain at an early stage.

The secondment will support CNCS and relevant stakeholders in assessing the scale and characteristics of the problem, identifying technical, regulatory and operational gaps, and developing practical recommendations adapted to the Dominican telecommunications ecosystem. It will also strengthen national capacity through knowledge transfer and cooperation between CNCS, the telecommunications regulator, operators and other relevant stakeholders.

Finland offers relevant experience in securing electronic communications and preventing caller ID spoofing. Building on exchanges initiated during the 2025 EU–LAC Digital Alliance study visits to Finland, the secondment provides an opportunity to translate Finnish and European experience into practical cooperation in the Dominican Republic.

The assignment may also identify opportunities for longer-term cooperation with Finnish actors, including potential follow-on pilots, technology partnerships, specialised advisory services and technical training. Any such opportunities shall be identified on a technology-neutral basis and remain separate from future procurement decisions.

Host Organisation



The **National Cybersecurity Center of the Dominican Republic (CNCS)** is responsible for coordinating and strengthening cybersecurity management at the national level and protecting critical information and telecommunications infrastructure. Its responsibilities include cybersecurity policy and coordination, incident response, stakeholder cooperation and the promotion of national and international cybersecurity standards and good practices.

For this assignment, CNCS will act as the host organisation and technical counterpart, coordinating access to relevant stakeholders and supporting the integration of findings and recommendations into national cybersecurity and digital resilience efforts.

Use of Digital Technologies

CNCS and relevant stakeholders use digital technologies for cybersecurity monitoring, threat analysis, incident response and institutional coordination. However, capabilities specifically related to caller identification and authentication, spoofing detection, fraudulent traffic analysis and call traceability remain limited, creating a need for specialised technical assistance and knowledge transfer.

Strategic and Stakeholder Context

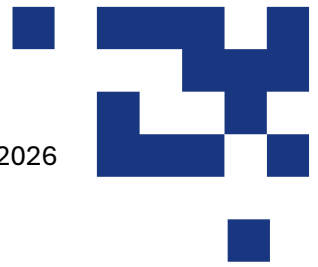
The assignment supports national efforts to strengthen cybersecurity, citizen protection and trust in digital communications, including the National Cybersecurity Strategy and relevant initiatives concerning telecommunications security, digital transformation and critical infrastructure resilience.

The CNCS interacts with the following organizations as key entities:

- Government Office of Information and Communication Technologies (OGTIC)
- **Dominican Institute of Telecommunications (INDOTEL)**
- Ministry of Industry, Trade and MSMEs (MICM)
- Ministry of Interior and Police (MIP)
- Private telecommunications operators and providers
- Academic institutions and research centers in ICT and cybersecurity
- Other relevant national security agencies and FDGT Finland, as the technical assistance and international cooperation partner.

Working Arrangements

The STE(s) will work primarily from the offices of CNCS in Santo Domingo and collaborate with relevant CNCS units and other national stakeholders, including the Computer Crime Investigation Division (DIDI) of the National Intelligence Directorate (DNI).



The designated focal points will support the STE(s)' institutional integration, facilitate access to relevant technical counterparts and stakeholders, coordinate information exchange and meetings, and support validation and follow-up of the assignment's findings and recommendations.

Focal points:

- Carlos Leonardo, Executive Director, National Cybersecurity Center (CNCS);
- Angela Noelia Martinez, Director of Strategy Coordination, CNCS;
- Yahaira Abreu, Coordinator of Cooperation and Interinstitutional Relations, CNCS; and
- Armando Díaz, Head of the Computer Crime Investigation Department (DIDI).

4. Objectives of the Secondment

Main Purpose

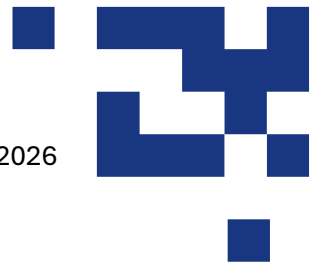
To support the National Cybersecurity Center of the Dominican Republic in the design, adaptation and implementation of a technical, regulatory and operational framework for the prevention of caller ID spoofing and related telephone scams, contributing to the mitigation of fraud and the strengthening of trust in telecommunications services.

Specific Objectives

The Short-Term Expert(s) shall:

- Assess the regulatory, technical and operational framework in place in the Dominican Republic for the prevention and mitigation of caller ID spoofing and related telephone scams.
- Transfer international knowledge and good practices, particularly from Finland and the European Union, related to technical standards, call authentication, regulatory models and public-private cooperation.
- Define technical and strategic guidelines for strengthening the prevention and mitigation of caller ID spoofing and related telephone scams, adapted to the institutional and technological context of the Dominican Republic.
- Strengthen the technical and institutional capacities of CNCS and other key stakeholders, promoting sustainable inter-institutional cooperation and knowledge transfer.

5. Methodology and Approach



The STE(s) will apply a mixed methodology that combines technical analysis, regulatory review, knowledge transfer and collaborative work, ensuring a practical, sustainable approach aligned with the needs of the host country.

Main Activities

The assignment will be structured around four complementary workstreams:

1. Diagnosis and assessment

- Assess the scale, characteristics and impact of caller ID spoofing and related telephone scams in the Dominican Republic.
- Review the relevant legal, regulatory, technical and operational framework.
- Assess the telecommunications ecosystem, including existing roles, responsibilities and cooperation between CNCS, regulators, operators and other relevant stakeholders.
- Identify priority technical, regulatory and operational gaps in the detection, prevention and mitigation of caller ID spoofing and related fraud.
- At the outset of the assignment, confirm with the host organisation the operational scope of the assessment, including whether it covers caller ID spoofing and scam calls affecting Dominican citizens and institutions domestically, the Dominican Republic's role as a potential source or transit point for outbound scam calls targeting foreign recipients, or both.

2. International good practices

- Present relevant Finnish, EU and other international approaches to preventing caller ID spoofing and telephone fraud, with particular reference to Finland's operator-level call detection and filtering model (developed by Traficom together with telecommunications operators), which identifies and blocks spoofed international calls without requiring a full caller authentication infrastructure.
- Review applicable technical standards and solutions for caller identification, authentication, spoofing detection and call traceability, including cryptographic authentication frameworks such as STIR/SHAKEN or equivalent, evaluated alongside lighter-weight, operator-level detection and filtering approaches, on a technology-neutral basis.
- Examine relevant regulatory, governance and public-private cooperation models and assess their applicability to the Dominican context.

3. Guidelines and recommendations

- Develop practical technical and operational guidelines for strengthening the prevention and mitigation of caller ID spoofing and related telephone scams.
- Recommend necessary regulatory, policy and governance measures.



- Propose a phased and sustainable implementation pathway adapted to the Dominican telecommunications ecosystem.

4. Capacity building and knowledge transfer

- Deliver targeted workshops and technical sessions for CNCS and other relevant stakeholders.
- Provide practical advice and knowledge transfer to designated technical and institutional teams.
- Support stakeholder dialogue and coordination around the proposed measures.
- Identify priority areas for future cooperation, pilots and technology transfer.

Division of responsibilities

STE: Lead the technical analysis, provide international expertise, develop recommendations, and prepare the agreed deliverables.

Host Organization: Provide information, coordinate meetings with key stakeholders, designate technical counterparts, and ensure institutional integration of results.

6. Expected Deliverables

- **Diagnostic Report:** A concise assessment presenting the key findings on caller ID spoofing and related telephone scams, the existing regulatory, technical and operational framework, and identified gaps, risks and priorities for action. The report shall explicitly scope whether it addresses caller ID spoofing affecting Dominican citizens and institutions domestically, the Dominican Republic's role as a source of outbound scam call operations targeting foreign victims, or both, to be confirmed with the host organisation during the inception phase.
- **Technical and Strategic Guidelines:** A practical set of technical, regulatory and governance recommendations, including a phased implementation pathway for strengthening the prevention and mitigation of caller ID spoofing and related telephone scams.
- **A presentation of the main findings** and achievements of the secondment to the host organisation, HAUS, the Finnish Ministry of Foreign Affairs and the Finnish Embassy.
- **Final report on the mission including:** Description of the activities carried out; Contribution of activities to achieve the above-mentioned objectives; Assessment of the potential for continued cooperation between Finnish actors and the partner organisation, and; Lessons learned, including recommendations for possible future temporary commissions.

7. Duration and Timeline



Planned Timing: The assignment is expected to commence in **January 2027**. The exact start date shall be confirmed in coordination with STE(s) and the host organisation.

Duration: The secondment shall have a maximum duration of **110 person-days**. The maximum of 110 person-days applies to the combined input of all proposed experts and backstopping personnel.

The assignment may be delivered through a combination of on-site and remote work; however, **no more than 30% of the total input may be provided remotely (including possible backstopping)**.

Tentative timeline:

Period	Activities	Deliverables
Weeks 1-2	Preparation, document review, detailed planning, and initial coordination with CNCS focal points.	None (preparatory phase).
Weeks 3-8	Technical-regulatory diagnosis: stakeholder consultations with CNCS, INDOTEL, DIDI/DNI and telecommunications operators; review of the legal and regulatory framework; assessment of the scale and impact of caller ID spoofing and related telephone scams.	Diagnostic Report (draft).
Weeks 9-12	Exchange of international good practices: presentation of Finnish and EU approaches to caller ID spoofing prevention; review of applicable technical standards and solutions, including STIR/SHAKEN and alternative frameworks; examination of governance and public-private cooperation models.	Diagnostic Report (finalised, incorporating stakeholder feedback).
Weeks 13-17	Development of technical and strategic guidelines, regulatory recommendations, and a phased implementation roadmap.	Technical and Strategic Guidelines (draft).
Weeks 18-21	Capacity building: workshops and technical sessions with CNCS and other relevant stakeholders; direct technical advice to designated teams; validation of draft guidelines with focal points.	Technical and Strategic Guidelines (finalised).



Week 22	Presentation of results and delivery of the final report.	Executive Presentation; Final Report
----------------	---	--------------------------------------

Evaluation note:

- When evaluating tenders, proposals that allocate a greater number of person-days (up to the maximum of 110) will be viewed favourably, as this indicates stronger capacity to deliver the full scope and outputs of the assignment. The score for person-days will be calculated proportionally using the following formula: **Person-days score = (Proposed person-days / 110) × maximum score**. Proposals offering 110 person-days will receive the full score, while lower allocations will receive proportionally fewer points.
- Certain tasks may be conducted remotely where this is duly justified, up to a maximum of 30% of the total input.** Remote work may be particularly suitable for analytical and drafting tasks, including document and regulatory review, analysis of technical and operational gaps, and the development of technical and strategic guidelines and recommendations.

However, given the nature of the assignment, a strong on-site presence is considered to add value throughout the secondment by enabling closer collaboration with CNCS and other stakeholders, facilitating access to relevant information, strengthening knowledge transfer, and allowing the experts to respond flexibly to emerging assessment needs. Stakeholder engagement, technical assessment, validation and capacity-building activities are therefore expected to be delivered primarily on-site.

Accordingly, proposals with a higher proportion of on-site work will receive a higher score for delivery modality. The score will be calculated proportionally as follows:

On-site score = (On-site person-days / total person-days) × maximum score

A proposal with 100% on-site input will receive the maximum score for this criterion. Proposals including remote input will receive a proportionally lower score, provided that remote input does not exceed 30% of the total person-days.

8. Budget and Payment

In the Budget Form (Appendix A), the tender shall include the proposed daily remuneration rate (item 1 below). **The same rate shall apply to all proposed input, including all expert input and organisational backstopping.** All other costs listed below (items 2–5) are covered by HAUS and shall not be included in the Budget Form



1. **Daily remuneration (to be proposed by the tenderer)**
2. International per diem allowance
3. Travel expenses to and from the assignment location
4. Accommodation expenses
5. Operational budget for local expenditure such as visa, phone contract, internet, workshops, translation and interpretation etc (to be determined on a case-by-case basis)

The terms of compensation follow the Finnish Government's travel expense reimbursement guidelines, and the conditions set out in the Contract.

Payment will be made monthly, based on actual workdays completed and receipts for the reimbursable expenses listed above.

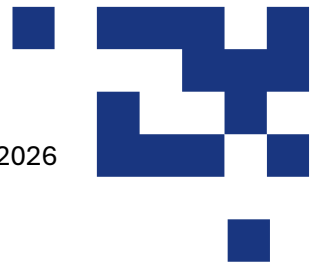
9. Expert Resourcing and Qualifications

The assignment may be delivered either by **one expert** covering all required areas of expertise, or by **two complementary experts** with clearly defined and jointly responsible roles. In the case of two experts, one shall act as **Lead Expert/Coordinator**, responsible for overall coherence, strategic direction and stakeholder engagement, while the **second expert focuses on specific thematic or technical areas** as defined in the tender.

The Lead Expert is expected to demonstrate strong capability in stakeholder coordination, institutional engagement, delivery oversight, and integration of outputs. Deep technical specialization in all technical domains is not required for the Lead Expert, provided these competencies are adequately covered by the supporting expert. **The proposed allocation of responsibilities and person-days between the two experts shall reflect their respective roles and the expertise they are expected to contribute to the assignment.**

Additionally, both delivery models may include **organisational backstopping support** from the experts' home organisation for different areas of expertise. Backstopping may support, for example, **specialised technical analysis related to caller ID spoofing, caller identification and authentication, network-level spoofing detection and call filtering, fraudulent telecommunications traffic analysis and call traceability; specialised regulatory or policy analysis, and other clearly defined expert inputs that can appropriately be provided remotely**. Such support shall complement, and not replace, the Lead/Sole Expert or Second Expert in the core implementation of the assignment.

Any backstopping arrangement must be **clearly defined in the Technical Form (Appendix C)**, including the **name of each backstopping expert, area of expertise, specific activities or deliverables supported, and allocated person-days**. A maximum of **two backstopping experts** may be proposed. Organisational backstopping is limited to **15 person-days in total**,



must be included within the overall ceiling of **110 person-days**, and shall be delivered entirely remotely.

CVs (maximum 3 pages each) of all proposed experts, including potential backstopping experts, must be included in the tender documentation.

Qualifications

- **Telecom and Caller Authentication Technical Expertise (Max 25 points)**

Demonstrated hands-on experience in one or more of the following areas: caller identification and authentication standards (e.g. STIR/SHAKEN or equivalent frameworks), spoofing detection and network-level call filtering, fraudulent traffic analysis, call traceability, or secure telecommunications network and signaling architecture. Experience should demonstrate practical technical work in telecommunications security specifically, not general cybersecurity alone.

- **Public-Sector Cybersecurity and Institutional Capacity Building (Max 20 points)**

Experience supporting public-sector organisations in strengthening operational cybersecurity capabilities through practical implementation, institutional process development, mentoring and operational support. Relevant experience may include CSIRT/SOC workflows, inter-institutional coordination mechanisms, and risk-based prioritisation of cybersecurity measures.

- **Regulatory and Policy Design in Telecommunications or Digital Security (Max 15 points)**

Experience developing or advising on regulatory, governance or public-private cooperation models related to telecommunications security, fraud prevention or digital and cyber policy, including translating technical findings into actionable regulatory recommendations.

- **Facilitation and Multi-Stakeholder Coordination (Max 13 points)**

Demonstrated experience designing and delivering capacity-building activities, including workshops, training and structured knowledge transfer, in complex institutional environments involving multiple agencies, regulators and private-sector operators.

The focus is on practical capability transfer, institutional learning, and stakeholder alignment that leads to sustained operational improvement, rather than one-off training delivery or academic instructions.

- **Emerging Market Experience (5 points)**

Proven experience working in emerging market contexts, preferably in telecommunications, cybersecurity or digital infrastructure.

- **Education (3 points)**

Advanced university degree (master's degree or equivalent) in telecommunications engineering, computer science, cybersecurity, information systems, technology law or a closely related field.

- **Language (8 points)**



- Full professional written and spoken fluency in English is required for eligibility (see Eligibility criteria) and is scored up to **3 points** in this component.
- Working or professional proficiency in Spanish is considered an additional asset, given its role as the primary working language of most host-organisation stakeholders and telecommunications sector counterparts, and is scored up to **5 points**.

10. Evaluation

The selection of the seconded expert(s) will be based on a combined **quality and price assessment**. The quality assessment will have the predominant weight to ensure the selection of a highly qualified expert(s).

	QUALITY 80% The raw quality score is 109 points (Expert Form 89 + Technical Form 20), which is converted to a weighted score of 80 points.
Basic Information	The quality assessment will account for 80% of the overall evaluation. It will be based on the information provided in: • the Expert Form (Appendix B), • the Technical Form (Appendix C, note max 10 pages), and • Expert CV(s) (supporting document; maximum 3 pages per CV).
Interviews	The Contracting Authority reserves the right to conduct structured interviews with the two (2) to four (4) highest-ranked tenderers following the preliminary written evaluation. The purpose of the interview is to: • Verify information provided in the tender • Assess spoken English proficiency and communication skills • Clarify specific aspects of the expert's experience or methodology where necessary The interview will relate only to evaluation criteria already defined in this ToR. Not all criteria must be revisited during the interview. Based on the interview, provisional quality scores may be confirmed or adjusted where justified. The number of tenderers invited to interview will be determined based on the distribution of preliminary quality scores.
Expert Form (Appendix B)	Each criterion listed under the <i>Required Expertise</i> section in this ToR will be scored up to the maximum points allocated to that criterion - according to the depth and relevance of the candidates' experience, as demonstrated in the Expert Form, and relevant CV(s), as applicable to the proposed resourcing model. (Total score: 89 points)



	The CV(s) should be concise, up-to-date supporting document(s) (maximum 3 pages each), highlighting relevant experience that complement the Expert Form.
Two-expert proposals	Tenders may propose either one expert covering all required areas of expertise or two experts whose combined qualifications fulfil the requirements. Each proposed expert will be scored individually against the published criteria. For two-expert tenders, the team score for each criterion will normally be based on the higher of the two individual expert scores (“best-of-two” principle). An expert’s experience may be taken into account for a criterion only where the expert has a substantive role and sufficient input in the relevant activities or deliverables. Tenderers shall clearly specify each expert’s responsibilities, deliverables and number of person-days in the Technical Form.
Backstopping	Backstopping experts are not scored as separate experts. Where the ToR permits specialised backstopping expertise to complement the proposed expert(s), it may be considered in assessing coverage of the relevant criterion. Its contribution and person-days must be demonstrated in the Technical Form.
Technical Form (Appendix C)	The Technical Form (maximum 10 pages) covers key qualitative and quantitative aspects of the tender and each of them will be scored up to the maximum points allocated to that criterion. The form covers: Understanding and scope justification (5 points), Proposed approach and methods (5 points), Number of person-days (2,5 points) and on-site/remote allocation (2,5 points), and Delivery modality (including the single-expert-plus-backstopping model or, if proposed, a two-expert model, and any backstopping arrangements) (5 points). (Total score: 20 points).
Minimum quality requirements	To be considered for contract award, tenders must achieve a minimum of 60% of the total quality score. Tenders failing to meet this threshold will not be considered for contract award.
Total quality score	Expert Form (Appendix B) 89 points + Technical Form (Appendix C) 20 points = 109 points Converted into a weighted value of 80%



	Weighted Quality Score = (Tender Quality Score / Maximum Quality Score) × 80
--	---

Indicative scale for qualitative evaluation criteria

The quality scores will be assigned based on the following indicative scale. The scale shall be applied to each qualitative evaluation criterion in light of the specific requirements of that criterion and the evidence requested in the relevant tender document. Evaluators shall consider, as applicable, the relevance, depth, specificity, credibility and completeness of the evidence provided, as well as its linkage to the assignment, required tasks and expected outputs.

Score range	Description
0–20% of max points	Very weak: The criterion is not addressed, or the information provided is largely irrelevant or unsupported. Required elements are missing or there is insufficient evidence to establish the tenderer's capability or suitability in relation to the criterion.
21–40%	Weak: The criterion is addressed only partially. Some relevant evidence is provided, but important elements are missing, insufficiently developed, weakly substantiated or only indirectly relevant to the assignment. Significant weaknesses or delivery risks remain.
41–60%	Satisfactory: The criterion is addressed to an acceptable level and the proposal demonstrates generally relevant capability, experience or approach. However, the evidence lacks depth, specificity, direct comparability or sufficient linkage to the assignment, tasks and expected outputs.
61–80%	Good: The criterion is addressed clearly and comprehensively. The proposal provides relevant and credible evidence, demonstrates a good understanding of the assignment and/or strong relevant capability, and establishes clear links to the required tasks and outputs. Any weaknesses are minor and do not materially affect confidence in delivery.
81–100%	Excellent: The criterion is addressed fully and convincingly, with highly relevant, specific and well-substantiated evidence. The proposal demonstrates substantial depth, strong understanding and/or proven capability directly applicable to the assignment, with clear responsibilities, results and links to the required outputs. No significant weaknesses are identified.

	PRICE 20%
Basic information	The tenderer shall indicate the proposed daily remuneration rate in the Budget Form (Appendix A).



	For the price assessment, only the daily remuneration rate will be compared across tenders, not the total price. The lowest rate receives the highest score (20 points). Other tenders will receive proportionally lower scores according to the ratio of their proposed rate to the lowest rate. The same daily rate shall apply for all services. Price Score = (Lowest Tender Price / Tender Price Being Evaluated) × 20
--	---

11. Eligibility Criteria

Eligibility criteria ensure that only qualified tenderers are considered, while evaluation criteria determine the quality and suitability of tenders. The required experience must be demonstrated by the **proposed expert(s) themselves** as part of their professional CVs and assigned roles, and cannot be fulfilled solely through organisational backstopping.

- **The Sole/Lead Expert** must demonstrate a **minimum of 5 years** of relevant professional experience in telecommunications security, cybersecurity, or public-sector digital systems. In case of a **two-expert proposal**, the **Lead Expert** must **meet this requirement in full**. The **second expert** must demonstrate a **minimum of 3 years** of relevant professional experience in the same fields.

For the purposes of this requirement, relevant experience refers to hands-on operational experience in one or more of the following areas: caller identification and authentication standards (e.g. STIR/SHAKEN or equivalent), spoofing detection and network-level call filtering, fraudulent traffic analysis and call traceability, secure telecommunications network or signalling architecture, or operational cybersecurity implementation in public-sector or critical-infrastructure environments, including incident response, CSIRT/SOC operations, or identity and access management.

- The proposed expert(s) must collectively demonstrate **proven practical experience** covering at least two of the following areas:
 - Caller identification and authentication standards, or spoofing detection and call filtering.
 - Fraudulent telecommunications traffic analysis and call traceability.
 - Regulatory or policy design for telecommunications security or digital fraud prevention.
 - Public-sector cybersecurity institutional capacity building, including CSIRT/SOC operations, incident response, or identity and access management.

In a single-expert proposal, the Sole Expert must personally demonstrate the required coverage. In a two-expert proposal, these competencies may be distributed across the proposed experts, provided that the team collectively



covers at least one telecommunications technical area (a or b) and either the public-sector institutional area (d) or regulatory area (c).

- The service provider is required to be a **Finnish legal entity** or other entity which has a **Finnish Business ID**
- This requirement reflects the mandate of the FDGT project to mobilise Finnish expertise and support cooperation between partner institutions and the Finnish digital ecosystem.
- The expert must be **fluent in English** (speaking and writing), with excellent drafting, analytical, and communication skills.
- **The tender includes all required documents:** Budget form (Appendix A), Expert form (Appendix B), CVs, and Technical Form (Appendix C).
- Full compliance with relevant data protection regulations, including GDPR, and adherence to the Principles of Conduct Clause outlined in this ToR.

12. Tender Submission Details

All proposals must be submitted electronically through the tender portal.

The tender must demonstrate that the service provider meets the **eligibility** criteria. **Only eligible candidates will be considered.**

Requested documents are:

- Budget Form (Appendix A)
- Expert Form (Appendix B)
- CV highlighting relevant experience (**note CV max 3 pages**)
- Technical Form (Appendix C, **note max 10 pages**)

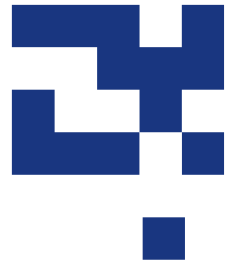
The minimum font size is 11 points. All documentation must be in English.

Tenders will be opened collectively after the submission deadline. Evaluation will then be carried out in accordance with the published criteria. Contracting will proceed following the completion of the evaluation process and the expiry of the appeal period.

Personal data contained in the submitted documents will be processed solely for the purposes of this procurement procedure. The documents will be shared with members of the selection panel as part of the evaluation process but will be retained only for as long as necessary for the purposes of this procurement, after which they will be securely deleted in accordance with applicable data protection requirements.

13. Questions during the Procurement

During the procurement process, all interested parties are encouraged to submit any questions or clarifications regarding the procurement process via the online system. All questions received



will be addressed as soon as possible. Please ensure that all inquiries are submitted within the specified timeframe indicated in the tender portal to allow for a timely response.

Only communication and contacts made through the Supplier Portal will be considered. The Contracting Authority is unable to respond to queries made otherwise, for example by telephone, mail or e-mail.

14. Reporting

The STE(s) will report to FDGT Project Manager and will maintain regular communication with the FDGT team throughout the secondment.

The STE(s) delivers a timesheet on the actual workdays and hours at the end of each month to the FDGT team.

15. Anti-Corruption

FDGT is committed to preventing and not tolerating any act of corruption and other malpractices and expects that all bidders will adhere to the same ethical principles.

16. Principles of Conduct Clause

Service Provider seeking to work with the Client (HAUS) shall adhere to the following principles:

- **Confidentiality:** Service provider must only use information solely for the purpose of performing their duties with the Client.
- **Business Ethics:** Service Provider are expected to uphold the highest standards of business ethics when collaborating with the Client
- **Transparency of Information Provision:** Service Provider must refrain from engaging in any fraudulent activities or misrepresenting information to influence the selection and contract awarding process in their favour
- **Fair Competition:** Service Provider should abstain from participating in corrupt, collusive, or coercive practices
- **Officials Not to Benefit:** The Service Provider guarantees that no official associated with the Client has received or will receive any direct or indirect benefit from the Bidder, the Service Contract or its award. Any violation of this provision will be deemed a breach of a fundamental term of the Service Contract
- **Data Protection:** Service Provider must comply with all relevant data protection laws and regulations, ensuring the confidentiality and security of any personal or sensitive data provided during the collaboration.



17. Rights reserved

This RFP does not obligate FDGT to complete the tendering/RFP process.

FDGT reserves the right to amend any segment of the tendering/RFP prior to the announcement of the selected STEs.

FDGT reserves the right to remove one or more of the services from consideration for this contract should the evaluation show that it is in FDGT's best interest to do so.

FDGT may, at its discretion, issue a separate contract for any service or groups of services included in this tendering/RFP.

FDGT may negotiate a compensation package and additional provisions to the contract awarded under this tendering/RFP.

FDGT reserves the right to debrief the tenderers after the completion of the process due to possible high volume of tenders and avoiding the compromise of the process.