**NGIatlantic.eu - 4th Open Call**

**NGIatlantic.eu 4th Open Call Duration**: 15 June 2021 until 15 September 2021, 17:00 CEST

The main goal of the NGIatlantic.eu Open Calls is to incentivize EU – US NGI teams to carry out experiments using EU and/or US based experimental platforms. This will take the form of funding to be provided through a cascade grant process for the EU counterparts of the teams formed.

## 4th Open Call Topic Priorities

**Priority coverage areas** and **expected scope** of the NGIatlantic.eu 4th open call**:**

**Topic 1: Strengthening trustworthiness and resilience of internet** – experimentation of results on the NGI call topics related to increasing trustworthiness and resilience of the internet.

**Topic 2: Greening the Internet: a Sustainable and Climate-friendly NGI** – experiments of results related to use case implementations of innovative internet technologies and transparency mechanisms on EU – US experimental platforms shown to: fight against the climate change with significant improvement of energy efficiency; carry out measurements to create awareness of environmental impact of the Internet; and promotion of technologies that help reduce the energy consumption and carbon emissions.

**Topic 3: Service and data portability** – this topic will address the challenge of personal data portability on the internet as foreseen under the General Data Protection Regulation and the data porting and service provider switching as foreseen in the proposed free flow of non-personal data regulation.

**Topic 4: Open Internet architecture renovation** – this topic will focus on experiments supporting communities of developers in ensuring Internet architecture evolution towards better efficiency, scalability, security, and resilience.

**Topic 5: Internet data sharing and interoperable services** – this topic will address the challenge of sharing network data siloed in different internet regions across geographic boundaries and enabling trusted Internet services by composition and orchestration of globally distributed services. Such services also may include network-level, and security and privacy related services that are critical to ensure a trusted and safe internet. Experiments related to such cross-domain data sharing challenges to enable cyber threat identification, risk assessment and incident management, and enabling secure and interoperable internet services are of particular interest. **Note: in contrast with topic 3, this topic relates to the role of data sharing for the purposes of cybersecurity, rather than for services / applications.**

**Please note this open call is open to all**, both existing (funded) projects in the NGI RIAs in these areas and new NGI experimenters.

## EXTENDED TOPICS DESCRIPTION

Formatted: English (US)



Co-funded by the Horizon 2020 Framework Programme of the European Union

**Topic 1: Strengthening trustworthiness and resilience of internet** - this topic will focus on experimentation of results on the NGI call topics related to increasing trustworthiness and resilience of the internet. These may include issues such as: identity (e.g., self-sovereign-identity), authentication and authorization; traceability; privacy and confidentiality related to personal and non-personal interactions or flow of sensitive information over geographic boundaries, including cryptographic solutions; transparency and accountability (e.g., certificate transparency); and federated, collaborative and/or decentralized technologies for supporting internet-wide e-identities with various levels of identification, reputation and trust, to serve as a basis for new business models for verifying and valuating personal and other sensitive data. Resilience issues may include approaches for monitoring, detection and mitigation to counter large-scale disruptions/failures or ongoing/impending cyber-attack/intrusions, and support for crisis situations; these may include techniques for resource redundancy and dynamic reconfiguration; network isolation and virtualization techniques; situational awareness, survivability and self-healing approaches. Proposers should pay special attention to the following dimensions: efficiency, interoperability, scalability, usability, deployability, sustainability, adaptability, standardisation and compatibility with the eIDAS and other national frameworks.

**Topic 2: Greening the Internet: a Sustainable and Climate-friendly NGI** – this topic will focus on experiments of results related to use case implementations of innovative internet technologies and transparency mechanisms on EU – US experimental platforms shown to: fight against the climate change with significant improvement of energy efficiency, carry out measurements to create awareness of environmental impact of the Internet, and promotion of technologies that help reduce the energy consumption and carbon emission. As background, the NGI Forward project has identified a Sustainable and Climate-friendly Internet as one of eight key topics that will set out a vision for a better, more human-centric future internet and inform the initiative's policy and technology research agenda going forward. The authors of the eight topics at DATALAB, Aarhus University, point out if more priority isn't given immediately towards the greening of the internet, including sustainability and controlling emissions, the carbon footprint of the global internet technologies will double by 2025. It is estimated that the global carbon footprint of the Internet and the supporting systems is already similar to the amount produced by the airline industry globally and that Indeed, optimal resource consumption and minimization of carbon emission is a great challenge for the Next Generation Internet. Data centers and networking devices consume significant amounts of energy. It is imperative to improve energy efficiency, both locally and at the Internet level. Currently, there is a significant lack of transparency of environmental cost, which should be urgently resolved given the vast scale of resource usage. There is a need to make digital infrastructure system not only more energy-efficient but also incorporate new sustainability metrics to reflect unaccounted externalities such as energy source, e-waste and life-cycle cost of equipment. Therefore, NGIatlantic.eu invites EU – US applicants to provide and experiment with transparency mechanisms and sustainability metrics on the environmental cost of the Internet. Identification and tagging of most resource consuming elements are also very important and urgent. On both sides of the Atlantic, there has already been some early research and innovation (R&I) projects and initiatives focussing on alternatives to improving energy efficiency to ensure the greening and sustainability of the Internet and of the economy relying on it. This topic welcomes the results from these EU activities to team up with US teams (or vice versa, with US teams twinning with EU teams) to carry out experiments in this vitally important NGI topic.

**Topic 3: Service and data portability** – this topic will address the challenge of personal data portability on the internet as foreseen under the General Data Protection Regulation (GDPR) and the data porting and service provider switching as foreseen in the proposed free flow of non-personal data regulation. The topic should cover the separation of data from the services provided to the end-users, with a view to ensure seamless combination of internet services and frictionless switching.

Formatted: Justified

Deleted: i

Deleted: the carbon footprint of the global internet technologies will double by 2025.

Deleted: that can

Deleted:

Deleted: and



Co-funded by the Horizon 2020 Framework Programme of the European Union

Attention should be paid to technological developments, standardisation of personal profiles, practical handling of data sets mixing personal and non-personal data, operational and business models, as well as techno-legal constraints and the simplification of end-user contracts and terms of use.

**Topic 4: Open Internet architecture renovation** – this topic will focus on experiments supporting communities of developers in ensuring Internet architecture evolution towards better efficiency, scalability, security and resilience. Auditing, testing and improving protocols and open-source software and hardware that are used to manage the Internet, with renewed design goals such as isolation of contingencies, redundancy and self-repair, disruption tolerance, transparency, better real-time behaviour and energy efficiency. Ability to roll-out at Internet scale should be assessed as part of the proposed solutions.

**Topic 5: Internet data sharing and interoperable services** – this topic will address the challenge of sharing network data siloed in different internet regions across geographic boundaries and enabling trusted Internet services by composition and orchestration of globally distributed services. Secure and privacy-preserving data sharing is particularly important to address the rising cyber threats and incidents that are increasingly global in nature with threat actors that may include nation-states and/or be distributed across geographic boundaries. Such cyber threats and incidents include advanced persistent threats (APTs), massive data breaches, internet-scale cyberattacks and disruptions (such as those targeted towards critical infrastructures), Intellectual Property theft, politically motivated misinformation campaigns, etc. Sharing of Internet data to support continuous monitoring and data-driven analysis is critical to identify impending/ongoing attacks, support traceback and attributions, and intelligently respond to Internet events. Geographically distributed Internet-enabled services when composed in privacy-preserving and secure manner provides socio-economic benefits to global population while allowing privacy sensitive or confidential information to flow across geographic boundaries. Such services also may include network-level, and security and privacy related services that are critical to ensure a trusted and safe internet. Experiments related to such cross-domain data sharing challenges to enable cyber threat identification, risk assessment and incident management, and enabling secure and interoperable internet services are of particular interest. Note: in contrast with topic 3, this topic relates to the role of data sharing for the purposes of cybersecurity, rather than for services / applications.

## Type of Proposals

**For open call 4, there is one type of proposal being funded, as shown below:**

| Proposal type | Description | Maximum Contract duration | Monitoring frequency | Funding range* |
|---|---|---|---|---|
| ST – Short-Term contributions | EU-US NGI experiment project with R&I activities. | 6 months **(note: this has been increased at the request of applicants)** | Monthly | €25,000 - €75,000 |

* Eligible Costs: Cost of personnel (inclusive of 25% overhead) and travel & subsistence (cost-reimbursement contracts).

**Guidance:** For projects applying in all topics, there are funding mechanisms provided by the National Science Foundation (NSF) in a similar funding range as provided to ST projects that the US teams

Formatted: Not Highlight
Formatted: Not Highlight
Deleted: Two types of proposals can be funded under the NGIatlantic.eu Open Calls, as shown below.
Formatted Table
Deleted: LT – Long term contributions ... [1]
Formatted: Not Highlight
Deleted: 3
Formatted: Not Highlight
Formatted: Font: Bold
Deleted: Fortnightly
Formatted: Not Highlight
Formatted: Not Highlight
Deleted: a) Experimental Platform interconnections, since these projects are dealing with the interconnection activities of already mature experimental platforms, there would be an expectation that these projects would probably best fit in the Short Term (ST) projects category. Please note
Deleted: already some
Deleted: SF



Co-funded by the Horizon 2020 Framework Programme of the European Union

can avail of, including the **NSF US-EU DCL 21-048**[2] – a new dedicated supplemental fund for existing US NSF grantees to team up with NGIatlantic.eu partners, if they are in successful NGIatlantic.eu applications. The DCL is open to active NSF-funded researchers within NSF's Computer and Network Systems Core[3] and Secure and Trustworthy Cyberspace[4] programs. Funding available for NSF grantee of up to $100,000 or 20% of original grant budget for max duration of one year (n.b. the duration must fall within the period of their existing NSF grant period). Please note that the applicants still must explain how their US partners will fund their activities (independently from the DCL) and the proposals will be evaluated and selected based only on this information. US partners must commit to their work even if they finally do not receive their funding through the DCL. All supplemental funding requests subject to NSF's merit review process. Please read the terms of conditions and requirements of the DCL carefully at https://www.nsf.gov/pubs/2021/nsf21048/nsf21048.jsp.

**4th Call timing:**

- Launch: 15 June 2021;
- Submission of Declaration of Honor (DoH) by 15 September 2021, 17:00 CEST, with the application;
- Deadline: 15 September 2021, 17:00 CEST;
- Evaluation: Each proposal will be evaluated by members of an External Pool of Evaluators (EPE);
- Notification of Outcome: Applicants will be notified on the outcome of their proposal within three months of the deadline.

**Additional Notes:**

- A signed Declaration of Honour (DoH) must be submitted by the EU coordinators along with the application.
- For US partners, a signed Letter of Support (LoS) must be submitted by the US partners and uploaded along with the application." A template of the Letter of Support and Declaration of Honour can be downloaded from the "Supporting documents" section below.
- If your proposal is successful, you will be contacted within 5-10 business days of notification to take the steps necessary to prepare and sign the contract for the funding. Please note that a deadline of 10 business days will be applied to confirm both EU and US coordinator's intention to take up the contract to enable the funds to be re-allocated to other successful applicants."

## Evaluation Criteria

Each proposal will be evaluated based on the 4-criterion given below, with a scoring from 1 to 10 and the weighting indicated:

Criteria 1: Soundness of the proposal and foreseen impact on the Open Call topic (30%);

Criteria 2: Technical excellence & adherence to the Open Call topics (30%);

Criteria 3: Experience and qualifications of the applicant (20%);

[2] https://www.nsf.gov/pubs/2021/nsf21048/nsf21048.jsp
[3] https://nsf.gov/funding/pgm_summ.jsp?pims_id=505671
[4] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709



Co-funded by the Horizon 2020 Framework Programme of the European Union

**Deleted:** . For example, see Supplemental Funding Requests to Conduct Experimental Research on the NSF-funded Platforms for Advanced Wireless Research (PAWR)[1]

**Formatted:** Hyperlink, Font: Bold, English (UK)

**Formatted:** Not Highlight

**Deleted:** However, this guidance does not preclude other project types and amounts being requested, if explained and justified.

**Deleted:** ↵
¶
¶
**The following proposals will be preferably selected for funding, as follows:**¶
**Category a:** minimum 2 proposals with a clear centre of gravity in Cat a. It is recommended to use the ST type for proposals that focus on this category. If proposals combine topics of Cat a and b, they can use the LT type;¶
**Category b (5):** minimum of 2 ST proposals with a centre of gravity in Cat b (5);¶
**Category b (1-4):** all topics 1-4 shall be covered by proposals, with expectation of 3 ST projects funded and 1 LT project funded (please note this 1 LT could be a combined project concerning category a and category b).↵
¶

**Deleted:** T

**Commented [JC1]:** check this

**Deleted:** two

**Formatted:** Font: Bold

**Formatted:** No bullets or numbering

**Deleted:** *

**Formatted:** Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0 cm + Tab after: 1,27 cm + Indent at: 1,3 cm

**Formatted:** English (US)

**Deleted:** *

**Formatted:** Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0 cm + Tab after: 1,27 cm + Indent at: 1,3 cm

**Formatted:** Irish

**Formatted:** Irish

**Formatted:** Irish

Criteria 4: Economics of the proposal (20%).

The final scoring and ranking will be automatically determined by averaging the scores provided by the 3 independent evaluators identified from NGIatlantic.eu's EPE.

## Who can receive financial support?

Field Code Changed

Private and public organisations of any size (not individual researchers) located within the EU Member States or Associated Countries and twinned with a US counterpart, as described above to carry out the activities proposed. Please note that the funding is limited to coverage of the work to be carried out by the EU team. For the US teams, please refer to the funding mechanisms of your US partners (e.g. National Science Foundation).

## Will there be more open calls?

Field Code Changed

Yes. In addition to this call, NGIatlantic.eu will launch 2 more Open Calls in the period November 2021 – April 2022 – this is the 4th chance to get your EU – US NGI experiment funded!



Co-funded by the Horizon 2020 Framework Programme of the European Union

## Supporting Documents

Full Open Call text as PDF file

Proposal template in pdf format (contains brief instructions and its use is mandatory)[5]

Proposal template in word format (contains brief instructions and its use is mandatory)

Template for the Declaration of Honor (DoH) to be signed by EU coordinator and letter of support(s) (LoS) to be signed by the US partner(s)[6]

Standard Contract for successful proposals (General Agreement and Annexes) [7]

FAQ

[5] Will be available when call opens.
[6] Will be signed by both EU (DoH) and US (LoS only) coordinators at application submission stage.
[7] Please have your legal departments review this contract template **at application stage**, as it will be a non-negotiable contract if the project is funded.

**Deleted:** both

**Deleted:** coordinator

**Deleted:** Cost-reimbursement contract

**Deleted:** Will be available for signature by the EU coordinator after signatures of the DoH

**Formatted:** Font: Bold





Co-funded by the Horizon 2020 Framework Programme of the European Union

**Page 3: [1] Deleted** **James Clarke** **15/06/2021 12:32:00**