[****](https://pixabay.com/illustrations/cyber-security-computer-security-1784985/)

**Call for Contributions on the 2019 BPF on Cybersecurity - NRIs**

Dear National, Regional and Youth IGF representatives,

The IGF Best Practices Forum on Cybersecurity is calling for input for its 2019 effort. We are soliciting input by 20 September 2019.

We are very interested in understanding national and regional specifics on the cybersecurity challenges we all face, and are looking for your assistance. The 2019 IGF Best Practices Forum on Cybersecurity is a multistakeholder group focusing on identifying best practices in operationalizing agreements on cybersecurity, such as the UNGGE Norms of 2015, and the Paris Call for Trust and Security in Cyberspace.

To provide additional background, the Best Practices Forum has developed and released a [Background paper on Cybersecurity Agreements](http://www.intgovforum.org/multilingual/filedepot_download/4904/1658). Your contributions will help develop our final outcome document, and enrich discussion on these agreements within the group and within the IGF.

You can assist in the BPF by sending us answers to any or all of the following questions. They are divided in two sets:

* General questions should be relatively easy to answer, and provide a strong contribution to the BPF. Thank you in advance for addressing these.
* Specific questions are focused on very specific areas of interest. We do not expect you to respond to all of them, but if you have the opportunity to discuss them in your NRI, we welcome your input.

Contributions will be listed on the IGF website, then be compiled and synthesized by the Secretariat, and further circulated on the BPF mailing list and to the community for comment and further work towards an output document for the BPF to be presented at the 14th IGF in Berlin, Germany.

You’re kindly requested to try to keep the contributions to no more than 2-3 pages, and to include URLs/Links to relevant information/meeting agendas/presentations/etc. When including specific examples or detailed proposals, those may be included as an Appendix to the document. Please attach contributions as Word Documents (or other applicable non-PDF text) and send to bpf-cybersecurity-contribution@intgovforum.org .

If you’re interested in the work of the BPF, you are invited to subscribe to the BPF mailing list at: [*https://intgovforum.org/mailman/listinfo/bpf-cybersecurity\_intgovforum.org*](https://intgovforum.org/mailman/listinfo/bpf-cybersecurity_intgovforum.org).

For any questions, you can reach out to the BPF Cybersecurity lead expert Mr. Maarten van Horenbeeck, the BPF’s co-facilitators, Mr. Ben Wallis and Mr. Markus Kummer or BPF Consultant Wim Degezelle atbpf-cybersecurity-info@intgovforum.org .

Thank you,

Markus Kummer

Ben Wallis

*IGF BPF on Cybersecurity co-facilitators*

**\*\*\* CALL FOR CONTRIBUTIONS \*\*\***

*The call for contributions is also published at* [*https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2019-contributions-nris*](https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-2019-contributions-nris)

**Questionnaire**

Your name and official role at the NRI you are responding for:

* Coordinator
* Chair or co-chair
* Member of the Steering Group/Organizing Committee/MAG of the NRI [describe which]
* Interested participant/observer in an NRI
* An NRI community member
* Observer on the NRIs mailing list

Your contact information (e-mail):

*General questions*

* Has your NRI organized a session on cybersecurity? Was it considered a priority session?
* For how many years has your NRI covered cybersecurity as a topic?
* What did the session address, or was covered in the session agenda? Were any implementation plans or policy proposals presented or discussed at your meetings, or discussed during intersessional work?
* What were the main outcomes, or work initiated out of this session?
* Does your NRI maintain any key messages on cybersecurity?
* Have you discussed international agreements on cybersecurity, such as the Paris Call for Trust and Security in Cyberspace, or the UNGGE norms?

*Specific questions*

* What projects and programs have you seen implemented to support the goals of any agreements you signed up to? Do you have any plans to implement specific projects?
* During our review, we identified a few key elements that were part of multiple agreements and seem to have more widespread support and/or implementation. Do you have views around the relative importance of these (e.g. by providing a ranked list), or are there any others that you consider to be significant commitments in these types of agreements?

	+ **Further multi-stakeholderism:** identify or support that cybersecurity depends on the presence in debate and coordination of all stakeholder groups.
	+ **Vulnerability equities processes:** the realization that stockpiling of vulnerabilities may reduce overall cybersecurity, and processes can be implemented to help identify the appropriate course of action for a government when it identifies a vulnerability.
	+ **Responsible disclosure:** the need to coordinate disclosure of security issues between all stakeholders, including the finder, vendor and affected parties.
	+ **Reference to International Law:** whether the agreement reflects on the importance of aligning international law.
	+ **Definition of Cyber threats:** whether the agreement proposes a clear or aligned definition of cyber threats.
	+ **Definition of Cyber-attacks:** whether the agreement proposes a clear or aligned definition of cyber attacks.
	+ **Reference to Capacity Building:** whether the agreement makes specific references to Capacity Building as a needed step to improve cybersecurity capability.
	+ **Specified CBM’s:** whether the agreement describes or recommends specific Confidence Building Measures.
	+ **Reference to Human Rights:** whether the agreement reflects on the importance of human rights online.
	+ **References to content restrictions:** whether the agreement discusses the need for content restrictions online.
* What has the outcome been of these agreements? Do you see value in these agreements either as a participant, or as an outsider who has observed them?
* Have you seen any specific challenges when it comes to implementing the agreement(s)?
* Have you observed adverse effects, or tensions from any of the elements of these agreements, where specifics may be at odds with intended end results? For instance a commitment that may seem like it improves cybersecurity at first sight or tries to fix one issue, but has effects that lead to a reduction in cybersecurity?

*Publication*

Contributions will be published on the BPF webpage and included in the BPF’s output document. Please inform us here, should there be any limitations on the publication of your contribution, and indicate what title, organisation or contact person could be used to identify your contribution.