RFI:	**RFP-ACT-SACT-23-29**
Reference:	Q & A #2
Date of Issue:	18 April 2023

The following questions were raised with respect to subject **RFI-ACT-SACT-23-36**

Responses are to provide clarification.

Questions	Responses
1. What technology requirements (if any) exist for the Cyber Coalition 2023 Exercise?	1. There are no technology requirements nor technology restrictions, as the expected level of integration between exercise infrastructure and the experiment on synthetic environments can be reduced to a minimum. Any resulting restrictions/requirements resulting from this study will have to be evaluated.
2. Is the Synthetic Environment required to be Open Source?	2. Not necessarily, as long the technology provides the necessary capabilities, functionalities and performances, and compares well with all other available options. In equal terms, open source is preferred.
3. Will the Synthetic Environment have any source code escrow requirements?	3. Not for the scope of this contract. Implications should be evaluated as part of the study.
4. From where (City/Country) will the Cyber Coalition 2023 Exercise be run?	4. Cyber Coalition is executed in Tallinn, Estonia, but using remote access for a number of functions. Any synthetic environment implementation can make use of the distributed capabilities, as long as the scope of the trial is achieved.
5. Will use of a Synthetic Environment require an on-premise hardware deployment.	5. This depends on the offered system architecture. This is not a requirement per se, depends on the used technology. The study shall address this topic and identify consequences.
6. If the deployment is SaaS-based, will there be any geographical requirement for the leveraged data center?	6. No requirements at this stage. The idea is to identify potential technologies, architectures and set-ups enabling achieving the objectives.
7. What IT Security Stack components does the Cyber Coalition 2023 Exercise require?	7. None for the scope of this study. A future implementation will need to consider NATO security domains and security policies and directives per security domain.

8. What OT/SCADA components does the Cyber Coalition 2023 Exercise require?	8. None
9. Which of the 16 Critical Infrastructure sectors (as defined by US DHS CISA) does the Cyber Coalition 2023 Exercise require?	9. None. This is a sector agnostic study, and should preferably be focused on military operations and infrastructure required to execute and conduct military mission tasks.
10. What processes does the Cyber Coalition 2023 Exercise require to be available?	10. None, at this stage.
11. What attack scenarios does the Cyber Coalition 2023 Exercise require?	11. This is an outcome of this study. The study shall identify any scenarios that will need to be considered/developed.
12. What user emulation data does the Cyber Coalition 2023 Exercise require?	12. This is an outcome of this study. The study shall identify any requirements (including user emulation) that will need to be considered/developed.
13. Can one of you please clarify if NATO is looking for “cyber for cyber” (training cyber operators using synthetic environments) solutions or “cyber for others” (training the rest of the operators to fight through and win in cyber-contested synthetic environments) solutions.	13. We consider operational activities in and through cyberspace, so both aspects can be included in the response.