

Joint DHS S&T/CSD-Netherlands Research in Cyber Security

Broad Agency Announcement (BAA) Call HSHQDC-17-R-B0004

NWO Joint U.S. – Netherlands Cyber Security Research Programme

Closing date: August 31, 2017

1.0 Summary

The Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD) and the National Cyber Security Centre on behalf of the Netherlands Ministry of Security and Justice (hereafter NCSC) and the Netherlands Organization for Scientific Research (hereafter NWO) (individually, an “Agency”, collectively, “the Agencies”) wish to encourage joint research activities in cyber security.

There exists an “Agreement Between The Government of the United States of America and the Government of the Kingdom of the Netherlands on Cooperation in Science and Technology Concerning Homeland and Civil Security Matters,” dated November 29, 2012, and a subordinated Project Arrangement (PA) 01-2013, titled “Cooperation in Cyber Security” (collectively the “Agreements”) between the Government of the United States of America, and the Government of the Kingdom of the Netherlands. This BAA solicitation/Call (HSHQDC-17-R-B0004) is a call issued against Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year International Collaboration Broad Agency Announcement (BAA), HSHQDC-17-R-B0001 (current issue). All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001 (current issue) apply to this solicitation unless otherwise noted herein. The “current issue” of the DHS S&T CSD 5-Year International Collaboration BAA HSHQDC-17-R-B0001 used herein refers to the latest issue posted in Federal Business Opportunities (FBO).

The cooperative activity to be pursued via this solicitation by CSD, NCSC, and NWO is the Technical Topic Areas as specified below. This collaboration will be jointly managed by CSD and NWO on behalf of the Agencies, but there will be parallel review processes in the U.S. and The Netherlands, where final selections, based on prioritized lists developed independently, will be agreed to jointly between the DHS Selecting Official and appropriate Agency officials from The Netherlands. Attachment 1 depicts the process for the cooperative activity that will result in both awards to performers and agreements between the two countries. There are two principles driving this process: 1.) while funding for researchers in The Netherlands and U.S. will ultimately be provided separately by the Agency appropriate for their location, the goal of this solicitation is to support joint research projects that leverage each nation's expertise; and 2.) by requiring the deliverables to be independently delivered to each of the Agencies, there will not be any exchange of intellectual property between the Agencies.

2.0 Background

Building on previous initiatives intended to foster stronger research links between The Netherlands and the U.S., the Agencies would like to strengthen collaboration between our nations' best cyber security researchers.

The challenges of cyber security are global and do not respect national boundaries. Solutions to the problems with which we are faced will need to be developed and implemented in a shared way to reflect this fact.

3.0 Technical Topic Areas (TTAs)

This BAA is soliciting for up to four year efforts for two unrelated TTAs, Industrial Control Systems/ Supervisory Control and Data Acquisition (ICS/SCADA), and Distributed Denial of Service (DDoS) attacks and the Domain Name System (DNS).

3.1 Industrial Control Systems/ Supervisory Control and Data Acquisition (ICS/SCADA)

Industrial Control Systems (ICS) and/or Supervisory Control and Data Acquisition (SCADA) systems control segments of the infrastructure critical to the smooth function of our society. These systems collect information from sensors and actuators about some physical environment and provide an operator interface which allows control and reporting. The physical environment could be a power plant, power-distribution network, water-treatment plant, manufacturing floor, petroleum refinery, or any other physical environment that requires control and data acquisition.

Technically the ICS and/or SCADA system is composed of information technology (IT) that provides the human-machine interface (HMI) and stores and analyzes the data. It may contain the logic necessary to operate the physical environment either autonomously or semi-autonomously. Although technically not part of the SCADA system, SCADA systems are connected to the sensors and actuators via a complex network of devices that may include any of the following: Front End Processors (FEPs), Intelligent Electronic Devices (IEDs), Master Terminal Units (MTUs), Motor Control Centers (MCCs), Programmable Logic Controllers (PLCs), and Remote Terminal Units (RTUs).

Because ICS and/or SCADA systems are largely composed of commercial-off-the-shelf technology (COTS) they inherit all of the common vulnerabilities, in addition to some vulnerabilities that are quite unique. Given the critical nature of ICS and/or SCADA systems, developing tools and techniques to address one or more of the following ICS and/or SCADA topics are of interest. Note, however, research on this TTA is not strictly limited to these areas of interests:

- a.** ICS Digital Data Collection and Analysis. Develop forensically sound methods of digital data collection and rigorous digital data analysis for Industrial Control System field equipment including Programmable Logic Controllers, Remote Terminal Units (RTUs) and other Field Input/Output equipment to include data stored in drives, memory, telemetry data and firmware that can analytically prove an ICS Cyber-attack affected the field equipment and created any consequence in the process controlled by the field equipment.
- b.** ICS/SCADA Vulnerability Assessment Tool. Create a specific ICS vulnerability assessment scanning tool for use at asset owners as well as a more aggressive version for system assessments that is extensible
- c.** ICS/SCADA Common Operating Picture (COP) Tool. Create a tool with live information feeds that provides a common operating picture of cyber threats to Critical Infrastructure that includes specific adversary analysis, vulnerability analysis, and integration with live reporting from control systems.

- d. Securing ICS/SCADA legacy systems. Create architectures, protocols, guidelines and other technologies or solutions to protect older, insecure ICS/SCADA systems. This research will enable owners of ICS/SCADA legacy systems to easily maintain outdated and unsupported systems and protect them against current and future threats and vulnerabilities.

3.2 Distributed Denial of Service (DDoS) Defenses

DDoS attacks can take many vectors and targets. Attack vectors of particular interest include DDoS attacks directed at critical services and those directed at the Domain Name System (DNS), in particular. The DNS has played a role in several recent attacks and developing tools and techniques to address one or more of the following DNS related DDoS threats and vulnerabilities are of interest. Note, however, research on this TTA is not strictly limited to these areas of interests:

- a. Protection of the DNS against DDoS attacks. Attacks on the DNS have been used to disrupt Internet service. If you can stop the DNS, you effectively stop most Internet communication. Therefore, a goal of this TTA is to secure DNS beyond DNSSEC implementation.
- b. Prevention of exploiting DNS to generate DDoS attacks. DNS has been used as both a reflector and amplifier for attacks on other sites. In this case, the objective is not to disrupt the DNS but instead to use the DNS as a tool to disrupt other services. Therefore, a goal of this TTA is to develop techniques, mechanisms and tools to prevent any DNS component from being exploited in a way that facilitates a DDoS attack.
- c. Understanding the mechanisms and methods DNS can be used to effect and mitigate Internet of Things (IoT) DDoS attacks. A goal of this TTA is to explore IoT DNS related DDoS attacks. This could include: exploring DNS as a mechanism to better understand and potentially mitigate IoT based DDoS attacks; studying DNS to determine how information about what IoT devices are present, and what those devices are doing, to prevent DDoS attacks; and studying how DNS may be used to exploit IoT devices to implement botnet-based DDoS attacks.

4.0 Structure of this BAA Call

Proposals submitted in response to this BAA are required to have teams composed of capable entities from both the U.S. and the Netherlands and are required to present a single, unified, proposal which describes a full program of work in both countries, including the disposition of intellectual property as agreed to by the proposal team. Proposals will then be evaluated subject to the criteria applicable to each Agency and selections (i.e., funding decisions) will be coordinated by the Agencies based on mutual interest and in accordance with their respective criteria. As selections are made, each Agency will be responsible for the acquisition documentation process in their country, and to support the generation of Technical Annexes to PA 01-2013. This solicitation, in conjunction with BAA HSHQDC-17-R-B0001, defines the DHS requirements for offerors in the U.S., and the Agencies in the Netherlands will release a companion call for proposals detailing the requirements required of applicants from the Netherlands. However, all deadlines will be the same for each country. Lastly, either both national elements of a joint project will be funded or none at all – there will be no funding for just one country’s component of any project.

The Netherlands companion solicitation to this BAA call may be found at the NWO Cyber Security website: <https://www.nwo.nl/onderzoek-en-resultaten/programmas/cyber+security>.

5.0 Eligibility

This BAA call will provide DHS the mechanism to fund the portion of the joint R&D program to be performed in the U. S. Thus, the eligibility of offer responses to this BAA call are limited to responsible sources in the United States of America, including any teammates, other than those from the Netherlands. Offerors are advised that their participation is subject to the foreign disclosure review procedures, applicable export control laws, and other applicable federal laws, regulations, and policies pertaining to foreign entities. It is the intent of research and development contracting to obtain a broad base of the best contractor resources from the scientific and industrial community, to include small businesses and as a result, no portion of CSD BAA HSHQDC-17-R-B0001 will be set aside pursuant to FAR Part 19.502-2. U.S. Offerors may include (but are not limited to):

- a.** Single entities or teams from private-sector organizations;
- b.** Government laboratories;
- c.** Federally Funded Research & Development Centers (FFRDCs), including Department of Energy National Laboratories and Centers, are eligible to respond to this BAA, individually or as a team member of an eligible principal Offeror, so long as they are permitted under a sponsoring agreement between the Government and the specific FFRDC.
- d.** Historically Black Colleges and Universities (HBCU);
- e.** Minority Institutions (MI);
- f.** Small & Small Disadvantaged Business concerns, including Women-Owned Small Business concerns, Veteran-Owned Small Business concerns, Service-Disabled Veteran-Owned Small Business concerns, and Historically Underutilized Business Zone (HUBZone) Small Businesses concerns; and
- g.** Any academic institutions or non-profits organizations not included in the above categories.

6.0 Funding available

The Agencies plan to make available enough funding to support up to five (5) joint research projects deemed selectable by the Agencies. Proposals must request funding for a new concurrent research activity in both The Netherlands and the U.S. [Contributions to existing funded research from other sources, or projects which are resourced in either country, are not allowed.] Proposals should have parallel activities in both the U.S. and The Netherlands, starting and finishing at the same time in both countries. The total funding for this joint BAA call is up to \$2,500,000 (approximately €2.3 mln.); that is around \$1,250,000 (approximately €1.13 mln.) provided in each partner country. Maximum funding per project per partner country is \$250,000 (approximately €226,000). Funding for the approved projects depends on the availability of funds in the budgets of both countries.

7.0 How to Propose/Apply

Offeror teams must select a lead organization to submit the joint proposal in each country (i.e., the U.S. and the Netherlands). The proposal content submitted in each country must be the same. Should there be any deviation, neither proposal will be evaluated. Pointers to proposal/application requirements are as follows:

- a. U.S. Offeror submission requirements are detailed in the “Special Instructions/Notifications for U.S. Offerors” below
- b. The Netherlands Lead Applicant is responsible for final submission of the joint proposal to the appropriate Dutch Agency Officials, which may be found at the NWO Cyber Security website: <https://www.nwo.nl/onderzoek-en-resultaten/programmas/cyber+security>.

8.0 Guidance on Proposal Preparation

Final responsibility for producing the content of the combined proposal is shared by the offeror teams involved in the collaboration, in both the Netherlands and the U.S. Proposals must have a unified, cohesive nature. For example, a single statement of work (SOW) must be proposed with a lead entity identified for each task. In addition, the cost proposal must present an aggregated roll-up of all costs, as well as separate cost proposals for the Netherlands and the U.S. entities, respectively.

9.0 Evaluation and Assessment

CSD will manage the DHS proposal evaluation process; and NWO will manage the review and assessment process (see <http://www.nwo.nl/en/funding/funding+process+explained>) on behalf of NWO and the NCSC. As such, non-U.S. foreign government personnel and non-U.S. foreign non-government personnel may participate in the selection process as peer/scientific reviewers of submitted proposals in accordance with the process administered by NWO. After CSD and NWO have determined which proposals/applications they deem selectable for funding, the DHS Selecting Official will discuss with NWO prior to making funding decisions. To the extent possible, the Agencies will endeavor to effect the same starting dates for the joint proposal/applications.

10.0 Response Dates

Event	Time Due	Date Due
Proposals Due	8:00 AM EDT	August 31, 2017
Notification of Proposal Selections	N/A	TBD

11.0 Intellectual Property

This section describes how the Government of the United States and the Government of the Kingdom of the Netherlands plan to address intellectual property pursuant to the joint research solicitation issued by the Agencies. Participants should in particular pay attention to guideline a and c below, and inform Agencies accordingly. In accordance with the joint research solicitation, the Agencies will not exchange any intellectual property pursuant to the joint research project with each other. Instead, the Agencies will select their respective Participants in accordance with the process in this BAA call. The Participants will jointly create intellectual property and the Participant in each country will deliver to their country-specific Agency, intellectual property pursuant to this joint research project with a minimum of government purpose rights. Government purpose rights is defined as the right to make use of the intellectual property, including, but not limited to technical data and computer software for the purpose of expanding homeland security technology and knowledge capabilities of each Agency by initiating and conducting cooperative research, development, and testing and evaluation activities for the exchange and sharing of information within the field of cyber security and information assurance, and including cooperative activities that secure current and future cyber and critical infrastructures in the areas of industrial control systems/supervisory control and data acquisition and defenses against distributed denial of service. Government purpose rights will not include commercialization. The three guidelines below will be implemented in awards made to Participants and reflected in the Technical Annexes between the Agencies:

- a. **Participants' Assertion of Data Rights:** To execute the joint research project, the Agencies will issue awards to the Participants. As required by the joint solicitation, the Participants are required to assert data rights, as appropriate, if there are any to be asserted. However, all awards will be pre-conditioned such that the Participants will afford the Agencies with a minimum of government purpose rights as defined above.
- b. **No Transfer of Ownership:** There will be no transfer of ownership of any intellectual property between the Agencies pursuant to each joint research project.
- c. **Grant of Intellectual Property Rights:** The Participants will be required to provide intellectual property rights to each other sufficient for the execution of the joint research project.

12.0 Deliverables

The awarded performers in each country will be required to independently and separately submit deliverables identical in content, format, and medium to their respective funding Agency. Accordingly, each performer must be cognizant and abide by the export control laws applicable to them.

13.0 Special Instructions/Notifications for U.S. Offerors

a. General Instructions and Information

- i. This BAA solicitation/call (HSHQDC-17-R-B0004) does not include a requirement for white papers and only requires the submission of proposals subject to the date identified in the “Response Dates” table above.
- ii. Procedures for submission of proposals in the DHS S&T Portal are provided in paragraph 10 of DHS S&T CSD 5-Year International Collaboration BAA HSHQDC-17-R-B0001. Note that offerors must complete the company/organization portal registration PRIOR to submitting a proposal for the first time. Ensure adequate time to complete the company/organization registration as delays in this process will not be authorization for late submissions of white papers. Company, or organization, registration information is located in paragraph 10.1 of DHS S&T CSD 5-Year International Collaboration BAA HSHQDC-17-R-B0001. In addition, each proposal requires registration in the portal. Information regarding white paper (not required for this solicitation) and proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001.
- iii. Offerors may provide multiple proposal submissions; however, each submission must be distinct and self-contained without any dependencies on other work of any kind, while providing an approach to meet all of the TTA objectives for every TTA.
- iv. DHS has a strong preference for open source licensing of software for all software developed and delivered and the licenses for all proposed software deliverables will have to be identified in submitted proposals as required for the Assertions Table (reference DHS S&T CSD 5-Year International Collaboration BAA HSHQDC-17-R-B0001 (current issue), Section 9.6.1.u). However, as an alternative to open source release, offerors may also offer a technical transition plan detailing a commercialization plan that explicitly identifies the consumer market(s) and market(s) adoption forecasts for the technologies developed.
- v. The Evaluation Criteria in DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001 [3] Section 11 “EVALUATION OF WHITE PAPERS AND PROPOSALS” applies.
- vi. As an Appendix to Technical Volume 1, which will not count against the page count, proposals must include a one page biographical sketch for each Dutch collaborator, as well as a one-page supplementary document describing the benefit of the U.S.-Netherlands collaboration.

b. Travel

- i. DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded efforts are expected to present. Projects will be required to provide a briefing, typically 20 minutes, and are strongly encouraged to provide demonstrations when appropriate. The PI meeting is typically 2.5 days and attendance at the full event is encouraged.
- ii. In addition to the annual DHS CSD PI Meeting, it is expected that the joint project will hold two meetings each year. It is expected that one project meeting would be held in the U.S. and one would be held in the Netherlands.
- iii. NWO and NCSC (coordinated and executed by the Dutch Cybersecurity Platform Higher Education and Research – dcypher) holds a periodic NCSRA Symposium, showcase for running cybersecurity projects that receive NWO-funding, where it is expected that also a subset of joint US-NL projects are presented.

- iv. Costs to travel to team locations at least twice per year (NL to U.S. and U.S. to NL) should be included.

c. Proposal Requirements

To be considered for award, offerors **MUST** submit a proposal, compliant with the aforementioned response date, in accordance with the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001 (current issue). Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001 (current issue) may be rejected. (Note: The cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count. This portal generated cover page is a different page than that identified in HSHQDC-17-R-B0001 Section 9.6.1(a).) The DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001 (current issue), Section 9 discusses proposal preparation and describes the required proposal content; however, in addition to the guidance in Section 9, the following special instructions are added:

- i. Maximum Page Count.
 - a. Volume 1 – Technical Proposals.
 - i. For any proposal submitted in response to this solicitation/call, Volume 1, the technical proposal, SHALL NOT exceed fifty (50) pages. This maximum page count of 50 pages includes all information required to be included in Volume 1 of any submitted technical proposal. Information required to be included in Volume 1, Technical Proposal, is outlined in:
 - 1. Sections 9.6.1(a) through 9.6.1(v) of BAA HSHQDC-17-R-B0001 (current issue); and
 - 2. Any additional proposal information required by Section 6.8 of this solicitation/call (HSHQDC-17-R-B0004).
 - ii. Any Volume 1, Technical Proposal, received in response to this solicitation/call exceeding the maximum page count of 25 pages WILL NOT BE EVALUATED AND THEREFORE, WILL NOT BE ELIGIBLE FOR AWARD.
 - b. Volume 2 - Cost Proposals. THERE IS NO PAGE COUNT LIMITATION FOR VOLUME 2, PRICE/COST PROPOSAL SUBMISSIONS. Information required to be included in any submitted Volume 2, Cost Proposal, is outlined in:
 - i. Sections 9.6.2(a) through 9.6.2(c) of BAA HSHQDC-17-R-B0001 (current issue);
- ii. Subcontractor Cost Submission: Referencing, BAA HSHQDC-17-R-B0001 (current version), Section 9.6.2.b.(6), if the subcontractor costs cannot be included with a prime’s detailed cost breakdown, then the prime contractor must stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor’s costs are provided separately as an attachment to an e-mail sent to CSD-2017-International-BAA@hq.dhs.gov. The subject line of the email shall say “Separate Subcontractor Cost Submission – [insert the proposal number assigned from the DHS S&T BAA Portal]”. The body of the email shall contain the following:
 - a. The prime entities name which should be the same entity that is registered in the DHS S&T BAA Portal;
 - b. A POC (name and phone number) from the prime entity; and
 - c. For each subcontractor proposal attached, include:
 - i. The name of the subcontractor for the subcontractor proposal attached; and

- ii. A POC (name and phone number) from the subcontractor whose proposal is attached.

The separate subcontractor cost proposal must be as detailed as the offeror's cost proposal and must be received at the location designated in the individual solicitation no later than the closing date and time specified by the solicitation. Note that email transmission time may vary depending on the file size of the attachment(s) included in the email. Therefore, ensure there is adequate time for receipt of the email and any accompanying attachments of the subcontractor(s) cost proposal(s) by the required closing date and time. Acceptance of the email submission is dependent upon the actual date and time the e-mail and any accompanying attachment(s) is RECEIVED by the in-box for CSD-2017-International-BAA@hq.dhs.gov. NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE.

Ethical Research: Project proposals must include an ethical considerations paragraph, and where applicable reach out to their institutional ethics committee or institutional review board.

d. Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation/call (HSHQDC-17-R-B0004) must be emailed to CSD-2017-International-BAA@hq.dhs.gov no later than 4:30 PM ET on August 25, 2017. Emails submitting questions are to include "Questions for Joint DHS S&T/CSD-Netherlands Research in Cyber Security" in the subject line. All questions and responses will be posted on the Federal Business Opportunities website <http://www.fbo.gov>. Questions will only be accepted and answered electronically.

e. Order of Precedence

Additional Information: In the event that any of the terms and conditions contained in this BAA solicitation/call (HSHQDC-17-R-B0004) conflict with terms and conditions included in DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0001 (current issue), the terms and conditions in this BAA solicitation/call (HSHQDC-17-R-B0004) shall take precedence.

14.0 Partnering/Teaming List

As a courtesy, DHS will compile a list of those offerors that wish to be incorporated on a list that are interested in partnering. All e-mail inquiries shall have "Teaming List – Reference BAA Call HSHQDC-17-R-B0004" included in the subject line and must be sent by July 31, 2017 at 8:00 AM EDT. This information will be made available to all potential offerors via a weekly posting as an attachment to BAA Call HSHQDC-17-R-B0004 on FBO. Given that this BAA Call is supporting joint research between the U.S. and the Netherlands, only entities in those countries will be listed. Therefore, if interested, please submit the information listed below to the Contracting Officer via email at CSD-2017-International-BAA@hq.dhs.gov.

- a. Country
- b. Entity name
- c. Point of contact name
- d. Point of contact e-mail address
- e. Point of contact phone number
- f. TTA(s) of interest
- g. Keywords for area of competency
- h. Website/URL
- i. A description of capabilities and teaming interest (maximum 200 words – DHS will truncate any content beyond this).

Attachment 1 – Cooperative Activity Process

The process for how the cooperative activity will be conducted by the Agencies, and supported by this BAA call, is depicted in Figure 1 and Figure 2.

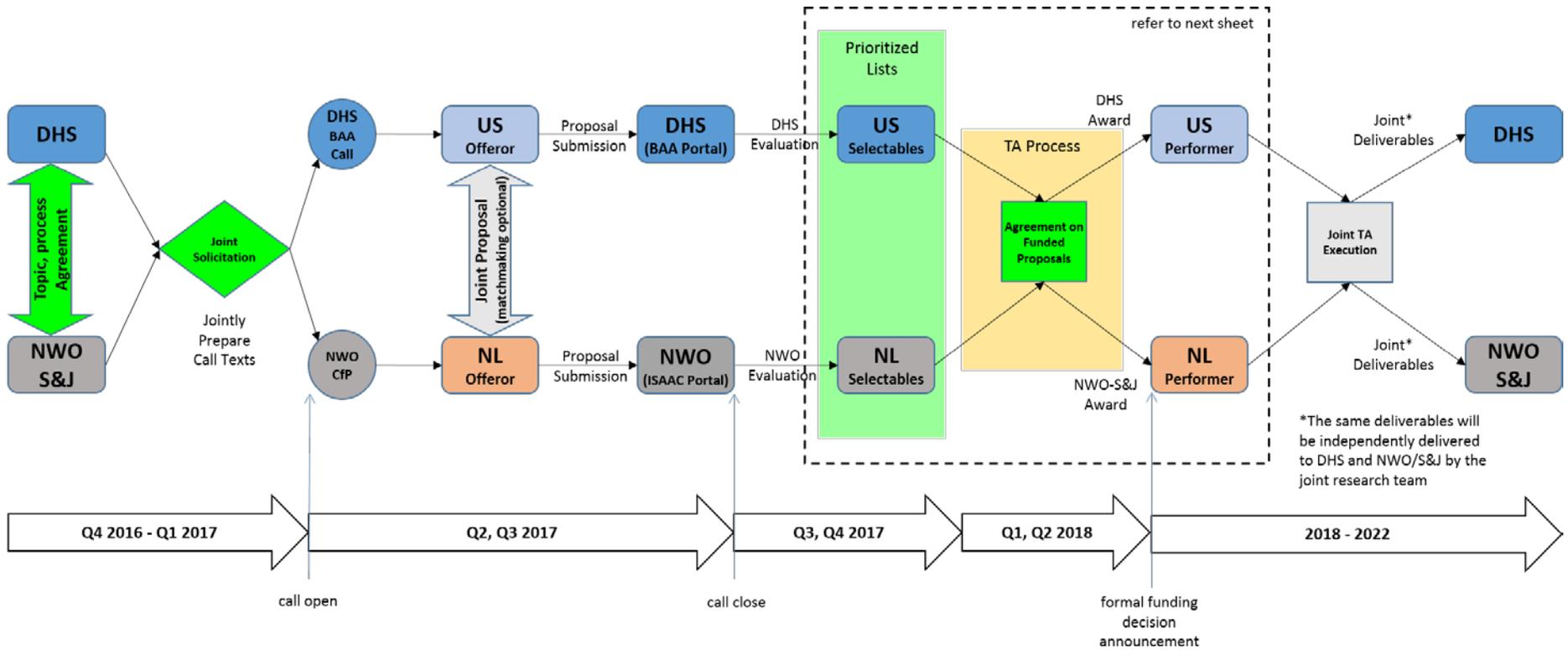


Figure 1: End to End Cooperative Activity Process

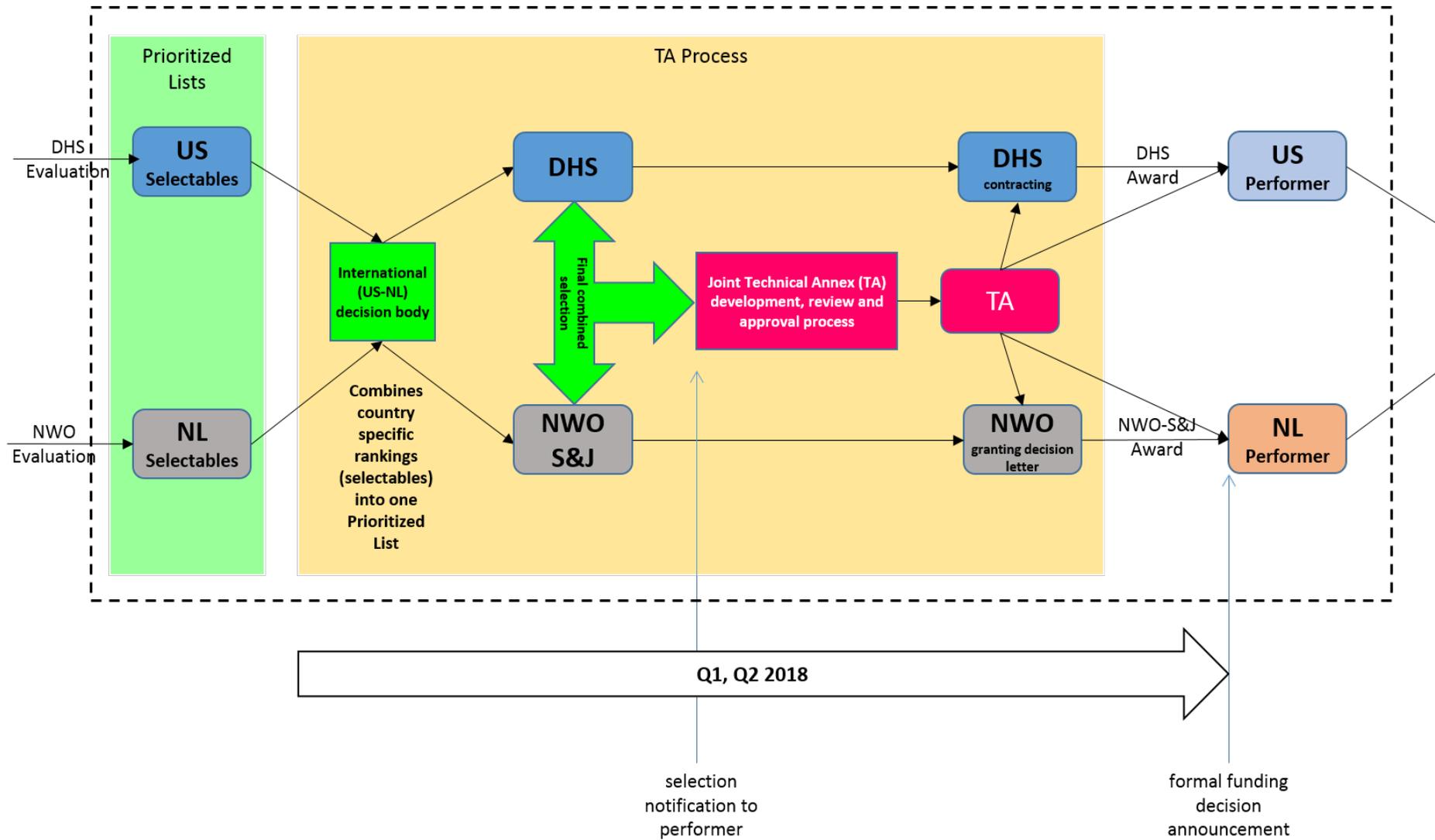


Figure 2: Performer Award and Country Agreement Process