

ANNEX E
CLARIFICATION REQUEST FORM

ADMINISTRATIVE or CONTRACTING					
Serial Nr	IFB BOOK	IFB Section REF	QUESTION	ANSWER	Status
A.1	Book I	Bidding Instructions, Section 2.11.5 Annex C, Section D	<p>Section 2.11.5 states: “If the Bid Closing Date is extended after a Bidder's financial institution has issued a Bid Guarantee, it is the obligation of the Bidder to have such Bid Guarantee (and confirmation, as applicable) extended to reflect the revised Bid Validity date occasioned by such extension.” Annex C, Section D says: “It is a condition of this letter of credit that the expiry date will be automatically extended without Amendment for a period of sixty (60) calendar days from the current or any successive expiry date unless at least thirty (30) calendar days prior to the then current expiry date the NCI Agency Contracting Officer notifies us that the Letter of Credit is not required to be extended or is required to be extended for a shorter duration.”</p> <p>Question: The bid guarantee needs some time of preparation. Therefore, it might be possible that the bid submission period is extended while processing the bid guarantee. However, the bidder assumes that no further action is required if the bid period is extended to fulfil the requirement in section 2.11.5 of the Bidding Instructions, as the bid guarantee is automatically extended unless the Bank is instructed by NCIA not to do so. Please confirm.</p>	<p>The Bid Guarantee validity shall be equal to that of the bid as stated in Section 2.10.1 of Book I; which is twelve (12) Months.</p> <p>The bank guarantee would automatically be extended as per the wording in Annex C, Section D. It is important for the Prospective Bidder to inform their bank per the Standby Letter of Credit in Annex C.</p>	Closed

NATO UNCLASSIFIED

A.2	Book II	Part 2 and Part 3	<p>Book 2 Part 2, Clause 13.2.2 states: “for each day of delinquency in achieving the deadline or milestone, fixed and agreed liquidated damages of 1% per day of the associated payment set forth in schedule of payments provided in Clause 11 of Contract Special Provisions.” Up to “15% of the value of each line item individually and an aggregate sum of all delinquent items not to exceed 15% of the value of the total contract”</p> <p>However ...</p> <p>Book 2 Part 3, Clause 38.1 states: “in lieu of actual damages the Contractor shall pay to the Purchaser, for each day of delinquency in achieving the deadline or milestone, fixed and agreed liquidated damages of .1% (one tenth of per cent) per day of the associated payment set forth in the Schedule of Payments provided in the Contract Special Provisions.” “to 20% of the value of each line item individually not to exceed 15% of the value of the total Contract.”</p> <p>Please can we clarify whether NATO mean 1% or 0.1% per day for the LDs and what is the percentage of the line items it would go up to, is it 15% or 20%?</p>	<p>In Book II Part II, Article 1 Alterations, Modifications and Deletions of the NCIA Contract General Provisions states under 1.4 “Clause 13 “Liquidated Damages” replaces Clause 38 “Liquidated Damages” of the NCI Agency Contract General Provisions.”</p> <p>Please note as stated in Article 2 Order of Precedence that Part II- The Contract Special Provisions takes precedence over Part III – The Contract General Provisions.</p>	Closed
A.3	N/A	N/A	<p>The tender regulations do not provide safeguards for delays due to COVID restrictions. It would be useful to include automatic safeguard mechanisms in the contract: if there were limitations to travel or work, not depending by the contractor, the contract times should be automatically extended.</p>	<p>Special Provisions regarding COVID-19 will not be implemented in Book II, The Prospective Contract. During the contract, should circumstances arise due to COVID, each situation will be treated on a case-by-case basis.</p>	Closed

ANNEX E

CLARIFICATION REQUEST FORM

PRICE					
Serial Nr	IFB Book	IFB Section Ref.	QUESTION	ANSWER	Status
P.1	Bidding sheets		In the „CLIN Summary” tab, in the "Delivery Destination" column, CLINs 7.2, 7.3, 8.2, 8.3, 9.2, 9.3, 10.2, 10.3, 11.2, 11.3, 12.2, 12.3, 13.2, 13.3 there is SHAPE as the location of Site Survey and Installation. Those CLINs are assigned to other locations. Should the “Delivery Destination” of those CLINs match the location of the planned IEG-C unit?	The referenced CLINs were erroneously assigned to other locations. The “Delivery Destination” column in “CLIN Summary” tab of the Bidding Sheets has been revised to indicate: “on-site (Annex B1)”.	AMD 4
P.2	BOOK I	Annex A-2, point 2	In BOOK I, ANNEX A-2 in point 2 it is stated that the working day is 7.6 hours for sites in Europe and 8 hours for sites in the USA. How many hours per working day should be assumed for Kabul?	An assumption has been added in Book I, Annex A-2, for Resolute Support Mission to indicate 12 hours (Mon-Thu) and 8 hours (Fri-Sun) for a 7-day working week. The Bidders have the choice to use different assumptions for their labour price estimate, as long as they describe their assumptions in detail, in the “comments” column of the “Labour” tab. The Bidding Sheets have been revised to include such column.	AMD 4
P.3	BOOK I	Annex A-2, point 5	In BOOK I, ANNEX A-2 in point 5 there is an information: „Bidders shall make sure that they have	The referenced content has been deleted from Book I, Annex A-2.	AMD 4

NATO UNCLASSIFIED

			filled all delivery dates in yellow". In the Bidding sheet „CLIN Summary" delivered to bidders there is not such a column but there is a column „Required Completion Date", which is already filled in and should remain unchanged. Should the above content in ANNEX A-2 be deleted?	The Bidders are requested to meet the required completion dates mentioned in the Bidding Sheets.	
--	--	--	---	--	--

Index	IFB version	IFB part	IFB section	Question	Answer	Status
T178	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, Page 158, section 6.8	This section refers to NCIA TN-1485 v1.1, 2012 which on turn requires strict conformance by a potential Security Target. Would a re-interpretation of the PP NCIA TN-1485 v1.1, 2012 and a re-design of its SFRs not lead to contradictions to ISO/IEC 15408 Common Criteria? Would the following: "...CC Evaluation Assurance Level (EAL) 4+ evaluation", based on this PP still be the correct terminology? Wouldn't the following be more accurate "somehow evaluated against a re-interpreted PP with revised SFRs"?	<p>Correct.</p> <p>This section recognises that some of the SFRs defined in NCIA TN-1485 v1.1, 2012 are too implementation-specific and consequently were not included within the SRS. It also adds a number of requirements that are based on assumptions in the PP, because although they are assumptions in the PP, they have to be met explicitly for the WG.</p> <p>This PP could be used in support of an EAL4+ evaluation, but note that if one chooses to do so, one needs to be aware of differences between the MAXLG and the WG deployment. There is no explicit requirement to use the PP, or be conformant with it, though it should be recognised that additional SFRs may be included, dependent upon the results of the Security Risk Assessment.</p>	Closed
T179	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, Page 158, section 6.8.1.2	<p>This subsection states that some SFRs in NCIA TN-1485 v1.1, 2012 needs to be revised. Are re-designed or revised SFRs reflected somewhere in this document?</p> <p>The first bullet states: "Where needed, the SFRs included in this section have been updated accordingly."</p> <p>Besides the generic name of the SFRs, where can someone find these updated SFRs? Is it up to the contractor to re-design SFRs? If so, to what extent?</p>	<p>The SFRs are contained in sections 6.8.2, 6.8.3, 6.8.4, 6.8.5 and 6.8.6, as indicated in section 6.8.1.6. The contractor is not expected to re-design these SFRs during bidding, though additional SFRs may need to be designed, dependent upon the results of the Security Risk Assessment.</p> <p>Also see the answer to T178.</p>	Closed
T180	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, Page 160, section 6.8.1.4	6.8.1.4 PP objectives and assumptions, which PP is meant here?	<p>The PP referred to is the one specified in NCIA TN-1485 v1.1, 2012 and contains Objectives and Assumptions. The authors have rewritten relevant Objectives into requirements, and have included those requirements in the sections that follow. For each requirement, the corresponding SFRs from TN-1485 are referenced. Some Assumptions from the PP have been rewritten to requirements, which are included in sections 6.8.2 and 6.8.3. Also see the answer to T178.</p>	Closed
T181	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, Page 160, section 6.8.1.5	<p>Regarding the statement "SARs are not included for the WG in this SRS."</p> <p>What is the purpose of this statement? Do the SRSs suppose to be a PP? If so, based on what?</p>	<p>Section 6.8 includes requirements taken from, or based on, the PP in TN-1485. By doing so these requirements become part of the WG SRS. The purpose of the statement "SARs are not included for the WG in this SRS." is to say that the authors do not explicitly add any of the PP SARs to the WG SRS. Instead, if the bidder decides to make use of the PP in TN-1485 for the purpose of a CC evaluation, the bidder shall select the relevant SARs themselves. Also see the answer to T178.</p>	Closed
T182	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, Page 162, section 6.8.2	<p>Source in [NCIA TN-1485 v1.1, 2012], where A.PKI_MODULE_EVALUATED and the corresponding OE.PKI_MODULE_EVALUATED referred to be applicable in SRS-6-376 which in turn requires an evaluation against US Government Basic Robustness PKE PP with CPV - Basic Package, CPV - Basic Policy Package, CPV - Policy Mapping Package, CPV - Name Constraints Package, PKI Signature Verification Package, Online Certificate Status Protocol Client Package and Audit Package at EAL 4.</p> <p>Is Version 2.75, July 24 2005 the latest version of the U.S. Government Basic Robustness PKE PP? This document is not listed in "SECTION 2 Applicable Documents".</p> <p>Is PKI Signature Generation Package intentionally ignored?</p>	<p>The latest version of the U.S. Government Basic Robustness PKE PP is Version 2.8, May 01 2007.</p> <p>It is an omission from the Applicable documents and will be added. The PKI Signature Generation Package should be included. (See SRS-6-238.)</p>	AMD4

T183	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 241	Section 8.3.1 lists several NIAP PPs. Would these PPs be required to be used by the contractor since these are referenced several times in APPENDIX C? Or is this only a suggestion? If so, what is the purpose of APPENDIX C?	Appendix C supports section 8.3.5.	Closed
T184	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 241	The list of referenced NIAP PPs require low assurance classes ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ATE_IND.1 and AVA_VAN.1. This implies EAL1! What is the benefit of an evaluation based on such low assurance? Potential vulnerabilities would not be exposed here but hundreds of pages of documents have still to be rendered.	The NIAP provide standardised PP to ensure achievable, repeatable, and testable requirements. In addition some PPs may be removed, dependent upon the results of the Security Risk Assessment.	Closed
T185	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 242	8.3.2 Target of Evaluation (TOE) Overview Regarding: "The logical sub-components are:". Why is the underlying hardware mentioned in the first bullet, if logical sub-components are supposed to be addressed?	The underlying hardware is part of the identified logical sub-component, which is relevant for the enforcing of the SFRs.	Closed
T186	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 242	Trusted Base Platform: Which OS are meant here? According to Figure 29 the TOE consist of several network devices, i.e. Firewalls, WG, MG etc.. Are all possible OS of these components supposed to be part of the TOE? Further, Figure 2 in section 1 depicts "WinOS" to be part of the IEG-C. Is this supposed to suggest WinOS to run on the IEG-C components?	See T1. No particular operating system is implied or inferred. Each of the IEG-C components may include the OS in their corresponding TOE. Figure 2 relates to IEG-C Management and Components. The depiction of "WinOS" is indicative and not normative.	Closed
T187	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 242	Quote: "The IEG-C is composed of a number of IEG-C components that contain logical sub-components, providing overlapping capabilities for the IEG-C components, which have different relevance for enforcing the security functional requirements (SFRs)." Is there any hint, about which SFRs are addressed in the sentence cited above? Further, is the IEG-C supposed to be one TOE? Since the headline states "Target of Evaluation"	Table 24 - Table 33 provide a breakdown of the SFRs that are addressed by each sub-component. The IEG-C will require an approval as a whole See also the response to T190.	Closed
T188	AMD3	SRS (Book II Part IV Annex A)	Book II, Part IV SOW Annex A, Page 243	Reference to Figure 22. What does this mean? Figure 22 deals with MG in DMZ Architecture. How does this relate to the topic regarding the TOE?	Figure 22 is the wrong reference. It should be Figure 29 - this will be corrected.	AMD4
T189	AMD3	SRS (Book II Part IV Annex A)	Book II, Part IV SOW Annex A, Page 243	What does "...part of the TSF provided by the operational environment." mean? How is it possible to provide TOE security functionality by the operational environment? Which SFRs are supposed to address "TSF provided by the operational environment"? Is this still related to ISO/IEC 15408 Common Criteria or something different?	The infrastructure platform may support some of the SFRs, dependent on the bidder proposed solution.	Closed
T190	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 243	Is it seriously feasible to define such large TOE composed of several separated systems in which sub-components run on different systems with potentially different trusted base platforms? Each component might have a different trusted base platform with different OS, besides some other components with several security software parts for each component. Is a security evaluation realistic within the given time frame? How is this reflected in the milestone plan?	The IEG-C will consist of a number of sub-components, some of which may have their own separate security evaluation/certification. The overall IEG-C will be presented for approval, including components and their certifications, as necessary	Closed
T191	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 246 & ff.	Structure of Table 24 to 33. What is the purpose of the separate presentation of IEG-C and its TSF sub components? Does it make sense that IEG-C has some lines unchecked? Referring to Table 23, all the other components are defined to be "IEG-C TSF sub-components" which implies that IEG-C TSF sub-components are already included in IEG-C.	The separate presentation of the IEG-C and TSF sub-components provides an indication of where the requirement is applicable - either to the whole IEG-C system or specific sub components. The IEG-C column should always be checked, as the other components are TSF sub-components as indicated in Table 23. This will be amended.	AMD4
T192	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 297	APPENDIX C: IEG-C Protection Profile What is the purpose of APPENDIX C: IEG-C Protection Profile? Is this supposed to be a Protection Profile related to ISO/IEC 15408 Common Criteria?	Appendix C supports section 8.3.5. (see also T183).	Closed
T193	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 297	Assuming APPENDIX C: IEG-C Protection Profile is a Protection Profile. Is an evaluation in terms of ISO/IEC 15408 Common Criteria possible? APPENDIX C: IEG-C Protection Profile uses references to several PPs/cPPs with different assurance packages (EAL1, EAL1+, EAL4+), is this not somewhat wrongly overdimensioned?	See T184. The PP is made to ensure achievable, repeatable, and testable requirements. But some PPs may be removed, dependent upon the results of the Security Risk Assessment.	Closed
T194	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 297	Assuming APPENDIX C: IEG-C Protection Profile is a Protection Profile. Where can one find the other chapters of a PP with rationals and clear statement about SARs and SFRs related to the TOE IEG-C?	These other chapters of a PP are not provided with the IFB.	Closed

T195	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A, Page 311	Just to give one example about mixing up of several PPs into something called "IEG-C Protection Profile": NCIA TN-1485 v1.1, 2012 requires FAU_GEN.1 with a basic level of audit. Besides this, [NIAP PP_ESM_AC_V.2.1, 2013] requires FAU_GEN.1 with a not specified level of audit. Is this intended? Was quality assurance done on this APPENDIX C to avoid contradictions?	NCIA TN-185 v1.1 specifies the required level of audit.	Closed
T196	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, p. 309 / p. 284 A. 1.5	Follow up question on response to T105. NCIA states labelling is not within IEG-C scope. Please confirm that NCIA is aware that if this is not clarified, an essential aspect to IEG-C is missing. IEG-C (Guards) will only securely block or pass unstructured data (e.g. eMails, PDF, XLSX, docx, jpg, avi) between HIGH and LOW domain if a NATO STANAG 4774/8 label is used and can be cryptographically checked by the IEG-C (Guards).	The IEG-C identifies the specifications for data labelling that are used to enforce the information flow control policy. Applications in the High and Low Domain are responsible for labelling the data according to these specifications in order to transition the IEG-C. There are many approaches that could be taken by the applications in the High and Low Domains to label their data, but this is outside the scope of the IEG-C project.	Closed
T197	AMD3	SRS (Book II Part IV Annex A)	Part IV SOW Annex A SRS, p. 309 / p. 284 A. 1.6	Which product will be used for data labelling on HIGH?	A variety of products may be used that produce conformant labels.	Closed
T198	AMD3	SRS (Book II Part IV Annex A)	Book II, Part IV SOW Annex A, SRS-4-105	Windows Server 2016 support ends 01/11/2022. Which product does NCIA need?	The extended end date for Windows Server 2016 is 1/12/2027. As noted in SRS-4-105, later versions of Windows Servers that are listed in the AFPL for the ON may be used.	Closed
T199	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, SRS-6-397, p.124	Why is NC3A TR/2012/SPW007959/03 the point of reference for the CIP? Shouldn't it be considered an outdated document that does not account for technological developments and where relevant COTS products have evolved to to adhere to various information assurance, etc. requirements?	While outdated this document is not superseded. Some SRS requirements have been adapted in previous IFB amendments.	Closed
T200	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, Section 3, p.7-8	May IEG-C be required to support directly connecting NATO SECRET to NATO RESTRICTED?	No	Closed
T201	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	C2 information - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the C2 information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T202	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Operational Planning information - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the Operational Planning information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T203	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Reporting information - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the Reporting information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T204	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Formal messaging - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the formal messages to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T205	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	File transfer - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on file transfer information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed

T206	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Web Service - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the Web Service information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T207	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Instant Messaging - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the instant messages to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T208	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Data base replication / synchronization of data - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the data base replication/synchronization of data to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T209	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Friendly Force Tracking Exchange - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the FFT information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T210	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	SMC - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the SMC information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T211	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Tactical Data Links - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the TDL information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T212	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Alliance Ground Surveillance Data - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the AGS information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T213	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Common Operational Picture- Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the COP information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T214	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Joint Intel Surveillance Recon Info - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the JISR information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T215	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	GIS - Does NCIA have documented schema definitions of all data objects sent from MS to NS that can be provided to the contractor upon award? Does NCIA have documented release rule-sets for data for the content inspection via web / mail guard?	NCIA can provide further details on the GIS information to the contractor upon contract award. Rule-sets for the content inspection via the web / mail guard will be dependent on the Low Domain that is connected to the IEG-C.	Closed
T216	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Formal messaging - Please provide an example of a formal messaging data object / message. What format does it have? How is it structured?	A formal message will be an SMTP/IMF message, with either a STANAG 4774/4778 confidentiality label, a FLOT label or keywords.	Closed
T217	AMD3	SRS (Book II Part IV Annex A)	Book II, P IV, SOW Annex A, p6. Data Flows	Reporting information - Please provide an example data object / message. What format does it have? How is it structured?	Reporting information may be carried in SMTP/IMF message, with either a STANAG 4774/4778 confidentiality label, a FLOT label or keywords. Reporting information may also be carried by application specific protocols that are mediated only by the firewalls.	Closed

T218	AMD3	SRS (Book II Part IV Annex A)	Bidders Question Response T5	In a response to bidders question T5, NCIA states "NCIA will sponsor". Does this mean NCIA will sponsor CC EAL4+ certification activities / costs for products outside of the approved budget for IEG-C?	In T5 by mentioning "sponsoring" the Agency did not mean to cover certification costs, but only assistance and guidance in the process. Apart from this, NCIA will not accept bids that go over the ceiling given in Book I	Closed
T219	AMD3	SRS (Book II Part IV Annex A)	Bidders Response T38	NCIA states that high-assurance guard is not required when connecting NATO SECRET to MISSION SECRET domain. This contradicts NATO Member State practices, SAA requirements and mission realities (e.g. ISAF, RSM) for federated mission networks that include e.g. Partnership for Peace and other non NATO entities within a MISSION SECRET where data classified NATO or national SECRET needs to be protected. Please confirm NCIA maintains its position.	NCIA maintains it's position. However if bidders offer a HAAG instead, that would more than welcome.	Closed
T220	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-116]	Is it possible to make the following changes to the SRS highlighted in RED? The IEG-C Web Guard component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source or an NTP server / NTP appliance in management network.	No - see SRS-4-52 (and SRS-4-51).	Closed
T221	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-13]	Is it possible to make the following changes to the SRS highlighted in RED? IEG-C_DEX SHALL offer an interface 'Core Services Management' on top of 'Communications Access Services Management' that SHALL support the following [...] • Telnet [IETF RFC 854, 1983] --> Suggestion to delete it as Telnet poses a major information security risk for a management network and for NS/MS	The requirements for the IEG-C remains. Note that the IEG-C can be configured to prohibit any protocol.	Closed
T222	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-214]	Is it possible to make the following changes to the SRS highlighted in RED? The IEG-C management workstation component SHALL be the Dell Optiplex 5070 SFF or other device optimized for information assurance / Cybersecurity.	SRS amended accordingly.	AMD4
T223	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-323]	Is it possible to make the following changes to the SRS highlighted in RED? The IEG-C SHALL be configurable from scratch using the DCIS orchestration and automation toolset. Alternatively, an installation process checking the integrity of installation source and/or a guaranteed 4-eyes configuration process is also acceptable.	No.	Closed
T224	AMD3	SOW (Book II Part IV)	SOW	For WP6 and WP11 the Contractor shall offer the hardware on a firm fixed price basis. As stated in the SOW, the list of the needed hardware components is not fix yet and shall be finalized in the design phase, before the conclusion of the PDR at EDC+3. Question: 1. On what basis shall the calculation for WP6 and WP11 be done?	PDR is not expected to change drastically the design of the system. The SOW statement was initially included to account for PFE, this has now been clarified in AMD4	AMD4
T225	AMD3	SRS (Book II Part IV Annex A)	SOW / SRS	There are no requirements regarding an IPS or at least an IDS. Questions: 1.) Is there a requirement to have an IDS for the IEG_C? 2.) How will the IEG-C integrate into a secure architecture that consists of IDS/IPS?	This will be covered by WP7 (integration of IEG-C in the Cyber Security Monitoring Capability)	Closed
T226	AMD3	SOW (Book II Part IV)	SOW Section 1.1.2.4	The gateway will mediate exchange of data for both "core" and "functional" services and will, whenever possible, conform to NATO STANAGs 4774 and 4778. Question: 3.) The term "whenever possible" gives room for interpretation. What is NCIA's understanding of this requirement and to which extent shall the bidder's solution conform to the NATO STANAGs 4774 and 4778?	It is NCIA's intention to allow only STANAG labelled data flows. However, until all services mark properly their data according to the mentioned STANAGs, a firewall custom-rule controlled data flow will be allowed. For the bidders, STANAG compliance of the IEG-C is mandatory.	Closed
T227	AMD3	SRS (Book II Part IV Annex A)	SOW Figure 3 (IEC Data Flows)	Remote Desktop is intended to control a system in MS by a user in NS. However, next to the data flowing from MS to NS (video-stream of the remote desktop connection) data needs to flow from NS to MS. Question: 1.) Is NCIA aware that mouse and key input would flow uncontrollable from NS to MS? Is that acceptable?	Yes.	Closed

T228	AMD3	SRS (Book II Part IV Annex A)	SOW Figure 3 (IEC Data Flows)	<p>File and web transfer shall both be bi-directional.</p> <p>Question: 1.) By what criteria can we release file and web transfer from NS to MS? 2.) Can we expect that all http communication is correctly labelled accord-ing to the STANAGs 4774 and 4778?</p>	<p>see T226. Rules and criteria will be set by NCIA operators. The IEG-C must support both automatic (STANAG compliant) and manual (firewall ruled) data flows.</p>	Closed
T229	AMD3	SRS (Book II Part IV Annex A)	SRS, Table 4, pg. 20 et.seq.	<p>Many protocols shall be filtered by the firewall only. The architecture connects both NS and MS switches directly with each other. Manufacturer and model of switches and firewall are prerequisites.</p> <p>Question: 1.) Is our assumption correct, that the listed / prerequisite hardware for switches and firewall components is checked and approved by NCIA to prevent data leakage from NS?</p>	<p>The listed/prerequisite hardware for switches and firewall components are to be used in the IEG-C. Verification and approval will be dependent on the final configuration.</p>	Closed
T230	AMD3	SRS (Book II Part IV Annex A)	SRS, Table 4, pg. 20 et.seq. Table 6, pg. 49 et.seq.	<p>According to SRS, the transmission of Full Motion Video shall be bi-directional and routed via Firewall. However, the SRS states in Table 6 that Full Motion Video should be mediated via the WebGuard.</p> <p>Question: 1.) How does this fit together? On what basis shall classified video stream be identified and blocked?</p>	<p>The Web Guard will support full motion video that is encoded in (or has been transformed to) XML. Some full motion video will not be transformed and this will be mediated only by the firewall. The firewall rules and Web Guard CIP will determine which video streams will be allowed.</p>	Closed
T231	AMD3	SRS (Book II Part IV Annex A)	SOW Figure 3 (IEC Data Flows)	<p>Web Browsing from NS to MS is indicated by an arrow pointing from NS to MS. However, to the bidder's understanding, the information flow must be from MS to NS. Additionally, no information may be sent from NS to MS.</p> <p>Question: 1.) Does NCIA want to prevent the input of classified data in a webpage hosted in the MS domain?</p>	<p>The configuration of the IEG-C will enforce the required information flows.</p>	Closed
T232	AMD3	SRS (Book II Part IV Annex A)	SRS, Table 4, pg. 20 et.seq.	<p>Tactical Data Links based on JREAP should be mediated by the firewall. However, the payload (Link 1, 11, 16, and 22) should be filtered by the WebGuard.</p> <p>Question: 1.) What's the idea behind the different mediation / filtering approaches for JREAP and payload? How should mediation by the firewall and filtering by the WebGuard be combined?</p>	<p>Some TDL protocols are expected to be transformed into XML, including an STANAG 4778 Metadata Binding, prior to transitioning the IEG-C. As a result, those protocols can be mediated by the Web Guard. The Web Guard filtering is layered on top of the firewall filtering.</p>	Closed
T233	AMD3	SRS (Book II Part IV Annex A)	SRS-4-43	<p>The only requirement listed for Voice is given in SRS-4-43.</p> <p>Question: 1.) Is Secure Voice over IP a requirement to be transferred across both domains?</p>	<p>Secure Voice over IP is not required to be transferred across the IEG-C between the High and Low Domains.</p>	Closed
T234	AMD3	SRS (Book II Part IV Annex A)	SRS Figure 8	<p>In the proposed architecture, there are a number of services that are being sent across the two sets of firewall.</p> <p>Questions: 1.) Is there any opportunity to optimize the design and ensure some of the applications flows can be sent across a CDS and filtered similar to the applications going through web proxy and web and mail guard? 2.) The bidder recommends that some of the highlighted applications that are sent across firewalls: FTP, Syslog, NTP to name a few should be reviewed. Is the bidder allowed to present an alternative approach in his proposal?</p>	<p>The proposed architecture allows for the addition of application-specific proxies and guards between the two firewalls. A CDS may be used between the firewalls as long as it meet the system requirements of the web proxy, web guard and mail guard.</p> <p>The bidder may present an approach that meets the system requirements. The IEG-C shall support all of the mandatory application protocols.</p>	Closed

T235	AMD3	SRS (Book II Part IV Annex A)	SRS Table 4	Database replication is needed for the Web Guard. Question: 1.) What databases need to be replicated?	The Web Guard will support database replication that is encoded in (or has been transformed to) XML. The actual databases that are replicated is not relevant for the IEG-C i.e there is not database-specific handling.	Closed
T236	AMD3	SRS (Book II Part IV Annex A)	SRS-4-129	Content Inspection Services (Identify, verify and transform content). Verifying the structure of data and removing/ blocking malicious content. In Web proxy - Looking for configured words/ phrases. White/ Black list attachment types. Question: 1.) Are there further detailed examples of content inspection policies required? Depending on the complexity required, the policies required will have an impact on delivery times. These policies will also impact performance and transit times across the devices.	The system requirement specification provides details of the contention inspection policy requirements.	Closed
T237	AMD3	Annex E Administrative and Tech CRs AMD 2	T2 & T23	It is not clear to us how NATO will regard bids that contain some non-compliance's against mandatory "SHALL" requirements. The response to CQ T2 states that "Proposals are excluded when they do not meet the mandatory requirements of the SRS" and "NCIA are willing to accept solutions and architectures based on COTS products that meet the mandatory requirements of the SRS" And then CQ response to T23 states "NATO will accept implementing the IEG-C with proven COTS products if they fulfil the security and functional requirements." Does this mean that solutions that do not fulfil the non-functional and other requirements will be acceptable?	The question includes contradictory statements. But as far as SRS requirements terminology is concerned and according to RFC 2119, SHALL or MUST statements are absolutely mandatory and non compliance will mean exclusion from bid consideration.	Closed
T238	AMD3	SRS (Book II Part IV Annex A)	SRS	The Palo Alto firewall is mandated and yet there are many mandatory and capability requirements placed up it. Would NCIA consider relaxing these requirements or place the firewall out of scope?	The firewall model is mandatory.	Closed
T239	AMD3	Annex E Administrative and Tech CRs AMD 2	T97	Please confirm that all sites have the same configuration requirements (as implied by answer to T97), i.e. once site 1 has been configured the same configuration can be used across all sites with just minor changes.	Confirmed	Closed
T240	AMD3	SRS (Book II Part IV Annex A)	SRS	There are various elements of a COTS solution and also those elements that are mandated that are beyond the control of suppliers, such as Operating Systems and Network Switches. Please can NCIA confirm that these elements can be considered outside the accreditation requirements?	No. But all COTS requested are already in operation in NATO networks.	Closed
T241	AMD3	Annex E Administrative and Tech CRs AMD 2	T95	NCIA answer to T95 does not provide clarification to the question asked as there is no visibility given in Book 1 section 4.5.2 of SRS requirement weighting. A weighting against each mandatory requirement would enable bidders to consider if the development work required to become compliant is financially viable.	This information is source selection related and is not releasable. However and as stated in the ref paragraph, sub-criteria are listed in order of importance and precedence.	Closed
T242	AMD3	Admin	Admin	Admin	-	Closed
T243	AMD3	Book I	4.5.2 Volume 1 - Technical	Please clarify if the maximum score of technical evaluation described by the third level sub.criteria included in paragraph 4.5.2.1.1 can be reached with the compliance of the proposal to all SHALL requirements in the SRS or with the compliance to all SHALL and SHOULD requirements.	This information is source selection related and is not releasable. However and as stated in the ref paragraph, sub-criteria are listed in order of importance and precedence. As far as SRS requirements terminology is concerned and according to RFC 2119, SHALL or MUST statements are absolutely mandatory and non compliance will mean exclusion from bid consideration. SHOULD statements are recommended, but non compliance can be accepted when justified.	Closed
T244	AMD3	SRS (Book II Part IV Annex A)	General	Please confirm if all SHALL requirements included in the Annex A - SRS are considered all mandatory requirements and the non-compliance to any SHALL requirements may result in the bidder disqualification.	As far as SRS requirements terminology is concerned and according to RFC 2119, SHALL or MUST statements are absolutely mandatory and non compliance will mean exclusion from bid consideration.	Closed

T245	AMD3	SOW (Book II Part IV)	Part 4	<p>Please provide the following reference documents which are not available from open source or NSO.nato.int web site.</p> <p>SOW-149, NCIA PDED 06.00.03 and AC/323 - D(2018)0009</p> <p>SOW-400, BiSC D-07-007</p> <p>SOW-467, AAP-44(A)</p> <p>SOW-551, NCIA AI TECH 06.03.01</p> <p>SOW-692, AC/35-D/2005</p> <p>SOW-702, AC/35-D/1017</p> <p>SOW-722, AD 070-005</p> <p>SOW-896, NAC AC/322-D(2007)0048</p>	reference documents will be provided. AAP-44A is replaced by AAITP-09.	AMD4
T246	AMD3	SOW (Book II Part IV)	Part 4	SOW-77, Please provide details of the ITSM tools	NCIA currently have BMC Remedy v9.1.02 for asset management, change management and service desk.	Closed
T247	AMD3	SOW (Book II Part IV)	Part 4	SOW-83, SOW-96, SOW 107, SOW-615, SOW-636 and SOW-638: Please provide details of the expected tools hosted by the purchaser as training may be required.	SOW requirement 83 and 96 are not related to tooling. Please explain what you'd like the Agency to clarify about it SOW-107: The Purchaser's CMDB tool is BMC Remedy SOW-615 and 636: The Purchaser's tools for the test case development and management are Zephyr Scale (plugin for JIRA) SOW 638: For requirements, the NCI Agency uses IBM DOORS. For defect management, the NCI Agency uses JIRA For test management, the NCI Agency uses Zephyr Scale (plugin for JIRA)	Closed
T248	AMD3	SOW (Book II Part IV)	Part 4	SOW-77, Please provide details of the ITSM tools	see T246	Closed
T249	AMD3	SOW (Book II Part IV)	Part 4	SOW-114, please identify all Purchaser's risks to project achievement	There is only 1 risk that is relevant and can be shared at the moment and that is related to accreditation delays due to NSAB (NATO CIS Security Accreditation Board)	Closed
T250	AMD3	SOW (Book II Part IV)	Part 4	SOW-196 and SOW 902, Please provide details of other systems, e.g milestone schedules and interface details and any specific details of the ITM project.	These details will be provided at the time of site surveys. Not much dependency is expected with the ITM project as IEG-C will not be sharing infrastructure with it.	Closed
T251	AMD3	SOW (Book II Part IV)	Part 4	SOW-239, please provide example of the System Operations Processes.	Current SOPs will be shared after Contract Award and the contractor is expected to update them.	Closed
T252	AMD3	SOW (Book II Part IV)	Part 4	SOW-2548 To enable to scope the work to develop the ICD please provide details of NEDS, AIFS and E-NPKI, such as reference documents and point of contacts and the template referenced in SOW-250.	There is no SOW 2548, but we think it refers to SOW-248, which was deleted	AMD4
T253	AMD3	SOW (Book II Part IV)	Part 4	SOW-645 Please explain the need for the data to be presented within a very limited timeframe as the purchaser will have active access to review test results through their tool.	This SOW requirement is put in place in case the test runs/cycles cannot be run directly in the tools (due to loss of connectivity, higher classification of the results, etc.). If the results are in the Purchaser's tools directly, then the requirement is met.	Closed
T254	AMD3	SOW (Book II Part IV)	Part 4	SOW-710, please identify the scope of the guidance and when this guidance will be provided.	The accreditation effort will be a mixed team (Contractor - Purchaser) activity. Guidance will be provided after Contract Award	Closed
T255	AMD3	SOW (Book II Part IV)	Part 4	SOW-762, The term "immediately" is unachievable, please redefine the period of notification.	Reporting shall take place right away after the Contractor establishes the fact, coordination will naturally take more time.	Closed
T256	AMD3	SOW (Book II Part IV)	Part 4	SOW-846 Please provide details of the Purchaser's internal change management process.	SOP 23.01 was added to references and will be shared with bidders.	AMD4
T257	AMD3	Book I	Par. 3.4.8.12.8	"Volume 1" seems to be a typing mismatch as para 3.4.8 is dedicated to Volume 3 and BCRM file states that the [BI – 3.4.8.12.8] requirement is for Volume 3. Could NCIA confirm the Volume 3 is correct?	the BCRM is an Annex to Part II which contains all volumes. Wording clarified in Book I.	AMD4
T258	AMD3	Book II	List of CLINs SoW Annex B	List of CLINs reports delivery of all site survey and installation in SHAPE instead of the sites listed in annex B. Could NCIA confirm sites of survey and installation are as per Annex B?	Delivery of all reports will be electronic and the project team will be at SHAPE. However conduct of site surveys and installations will be at each site respectively. Bidding sheets adjusted accordingly.	AMD4
T259	AMD3	SOW (Book II Part IV)	SoW para 3.2 SoW Annex B	In annex B Decommissioning (wp 4) is supposed end up 4 months after FSA (wp 3) while according SoW para 3.2 it seems that the decommissioning activity must end one month after FSA. Could you please clarify?	WP4 can be concluded up to 4 months after FSA. The contractor is free to choose to perform earlier after agreement with the purchaser, so as to optimize resource utilization.	Closed

T260	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-101]	According to requirement "The IEG-C Web Proxy component SHALL be an appliance or deployed on a physical server", would NCIA accept a solution where Web Proxy and Web Guard are hosted on the same physical server?	Yes, we would consider it	Closed
T261	AMD3	SOW (Book II Part IV)	Requirement C.3/Software Licenses	Can you please confirm that for the SW listed in C.3 the contractor will not have to source the SW licenses?	Confirmed	Closed
T262	AMD3	SRS (Book II Part IV Annex A)	SRS-9-6] and [SRS-3-102]	With reference to requirement [SRS-3-102] and the possibility to support 10GbE, does this apply also to the network interfaces defined in requirement [SRS-9-6], therefore management users?	Yes	Closed
T263	AMD3	SRS (Book II Part IV Annex A)	SRS-4-67]	The switch Dell N1124T is currently "End of Sale". A comparable/improved version could be Dell model N1524, in the configuration with: 24x 1GbE + 4x 10GbE SFP+ fixed ports, Stacking, IO to PSU airflow, AC. Would NCIA accept that model?	Yes. SRS amended to allow equivalent/current model, that meets the AMD4 requirements of the SRS	
T264	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-109]	Could the RDP proxy be deployed on a Virtual Machine, on a physical server where also other functions (Web Guard, Mail Guard etc.) are also running?	Yes	Closed
T265	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-10]	Regarding the STORAGE resources, would NCIA accept: a)a traditional Storage appliances connected through Fiber Channel? Any brand/model required? b)a Software Defined Storage solutions such as vSAN? c)any other storage requirement to be considered?	Yes to all options, as long as they meet the other requirements of the SRS as well.	Closed
T266	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-147]	Regarding horizontal scalability, would NCIA accept introducing a Load Balancer? If yes, what brand/ Model?	Yes to introduction of a Load Balancer. Any model as long as they meet the other requirements of the SRS as well.	Closed
T267	AMD3	SRS (Book II Part IV Annex A)	SRS-5-323	DCIS is an external domain from IEG-C system. Could you please elaborate the meaning of "configurable from scratch using DCIS orchestration" ?	This will be defined during site surveys.	Closed
T268	AMD3	SRS (Book II Part IV Annex A)	SRS-5-329SRS-5-331	What is the meaning of "multiple instances in parallel" ? Could you please elaborate on seamless transition from Primary to alternate IEG-C?	There may be two (2) IEG-Cs deployed between the High Domain and the same Low Domain for redundancy. When traffic is switched from one IEG-C to another IEG-C there should be no impact for users or administrators. For example, both IEG-Cs should be enforcing the exact same policies.	Closed
T269	AMD3	SRS (Book II Part IV Annex A)	SRS-9-36	Windows server 2016/2019 does not support SNMPv3 but IEG-C components must support SNMPv3. How can this be achieved ?	This is for the bidder to advise.	Closed
T270	AMD3	SRS (Book II Part IV Annex A)	SRS-5-46	Is it an average of less than two (2) failures per 1000 hours of IEG-C operation over a longer period of time, or should it be read as one (1) failure in 1000 hours moving window ?	Both are acceptable.	Closed
T271	AMD3	SRS (Book II Part IV Annex A)	SRS-5-48	Is the "two (2) failure every 7000 hours" calculated per IEG-C instance ?	Yes	Closed
T272	AMD3	SRS (Book II Part IV Annex A)	SRS-5-150	In the context of horizontal scaling, what does the management overhead refer to ? Is it physical equipment, is it resource usage or user work load ?	It refers to the management of the WG guard - e.g. the administrator work load.	Closed
T273	AMD3	SRS (Book II Part IV Annex A)	SRS-5-152SRS-5-234	This requirement is subjective. Can NATO further clarify how a 'high degree of learnability' is measured?	Requirements deleted	AMD4
T274	AMD3	SRS (Book II Part IV Annex A)	SRS-4-102	JREAP is no longer a firewall requirement, it became a Web guard requirement with AMDT 3. Is it correct ?	JREAP has been removed from SRS-4-102.	AMD4
T275	AMD3	SRS (Book II Part IV Annex A)	D.5.1.3 - D.5.1.4	The content of the six (6) key button mouse is a copy of the keyboard. Could you please provide the part number for the mouse ?	The mouse details will be updated. Now specific part number is specified.	AMD4
T276	AMD3	SOW (Book II Part IV)	Table 2: Project Milestones B.2.2.4. Milestones	There is a discrepancy between Table 2: Project Milestones System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT) EDC+17mo and B.2.2.4. Milestones System Integration Testing EDC+13mo Please clarify which is the deadline for System Integration Testing	milestones corrected in SOW	AMD4

T277	AMD3	SOW (Book II Part IV)	Table 2: Project Milestones B.2.3.4. Milestones	There is a discrepancy between Table 2: Project Milestones Deployment Authorization (DA) EDC+20mo and B.2.3.4. Milestones Deployment Authorization EDC+17mo Please clarify which is the deadline for Deployment Authorization.	milestones corrected in SOW	AMD4
T278	AMD3	SOW (Book II Part IV)	[SOW-585] Ch 8.2 TVV Activi	Can You please provide the TV&V Process Definition and Execution Document (PDED) ?	Reference will be provided	Closed
T279	AMD3	SOW (Book II Part IV)	[SOW-636] Ch 8.4 Tools	Can You please identify the Purchaser test management and automation tools ?	please see T247.	Closed
T280	AMD3	SRS (Book II Part IV Annex A)	SRS-5-153, SRS-5-235	SRS-5-153 and SRS-5-235 requirements state 80% success rate - can the prime provide further clarity on this or is this a question for NATO?	Requirements stand as they are.	Closed
T281	AMD3	Book I	3.4.8.7.1	The Initial Project Implementation Plan should include an initial Project Master Schedule (PMS). According to BOOK II Part IV, SOW-145, the PMS needs to be in Microsoft Project Format but the bid package (including the Initial Project Implementation Plan) needs to be a PDF file. Is it acceptable that Bidder attaches a PMS Microsoft Project file to the bid package?	The PDF is required (for redundancy reasons) and a MS Project native file is desirable.	Closed
T282	AMD3	Book I	3.4.8.6	Is it acceptable that the Project Team (including Key Personnel) will consist of Contractors employees working under both: employment contract and a B2B cooperation?	NCIA will award the contract to 1 prime. The prime contractor can choose which subcontractors to employ, as long as they come from the 28 Nations that funded the project. Please view Book I, Section 3.3.4; Section 3.3.8.2 and Certificate B-9 regarding subcontractors.	Closed
T283	AMD3	Book I	3.4.6.7.10	According to the point 10.3.10 of Book II, SOW, the Security Test and Verification Report (STVR) template will be made available for the Contractor after the Contract Award. Should the Contractor provide an initial STVR with the bid documentation package? If yes, then what kind of information is expected to be provided in the document before the template can be shared?	no initial STVR is required. Book I will amended to clarify.	AMD4
T284	AMD3	Bidding sheets	Part 1 – Schedule of supplies and services Section 3, Table 2	What is the required completion date for each of the CLINs of WP4 Decommissioning Legacy Equipment? Amendment 2 Book II – The Prospective Contract, describes the Required Completion Date of CLIN14.1 to EDC + 6 Months and CLIN 14.2-14.3 as EDC +27 Months. According to the answers to the clarification questions and Book 2, Part IV, Table 2 the required completion date should be FSA +4 Months.	Milestones changed in SSS and SOW. All WP4 CLIN latest delivery dates have been moved at FSA+4. But if it suits the Contractor planning and after agreement with Purchaser, these can be concluded earlier.	AMD4
T285	AMD3	SOW (Book II Part IV)	[SOW-711], [SOW-717]	The SISRS and STVP documents, should be prepared with reference to Security Mechanisms from NS Reference Baseline, that will be shared with the Contractor after the Contract Award. Is it acceptable that the initial versions of the SISRS and STVP will not contain all the requested information?	Yes. Only for bidding purposes security mechanisms will not be required.	Closed
T286	AMD3	SOW (Book II Part IV)	[SOW-634]	According to this SOW, Annex C of the SOW should contain NATO CIS security regulations, but this Annex describes the Purchaser Furnished Equipment, not CIS security regulations. Is this reference correct?	reference corrected in SOW (Section 2)	AMD4
T287	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-156]	Integration of HPE OneView and HPE iLO or Dell iDRAC are not applicable to altetnative solution architectures and favor only vendors part of the original IEG-C reference architecture. Suggestion to delete or remove SHALL requirement	The requirement is still applicable.	Closed
T288	AMD3	SRS (Book II Part IV Annex A)	[SRS-3-9]	[...] The Protection Services consists of the following three atomic services: Intrusion Detection Services [...] Does the IDS relate to the product capabilities of the PA-3260 Firewall?	Intrusion Detection Services will be provided by the NCSC monitoring capability.	Closed
T289	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-145]	Capability appears to favor single product and is directly associated with "*****" capability. Suggestion to delte or make optional allowing for alternative solutions	SRS amended	AMD4
T290	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-7]	How is the data flow for UDP and TCP in Figure 8 IEG-C Network Level System? Which UDP and TCP packets are needed? Information is not provided in Table 4: Protocols Supported By the IEG-C	The data flow is determined by the IEG-C and the corresponding higher level protocol e.g. to determine the flow through a proxy or guard. UDP and TCP packets requirements as as per the cited references.	Closed

T291	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-5] [SRS-4-226]	For security reasons requirements for graceful shutdown could not be initiated by some IEG-C COTS components and as such this requirement favors specific vendor. Suggest to delete or soften requirement	SRS amended	AMD4
T292	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-303]	Please specify what you mean by "the platform"	The "platform" is the IEG-C. SRS will be updated to clarify this.	Pending
T293	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-303]	Please specify how throughput increase by 10% will be measured	The 10% increase will be measured as a 10% increase in size and a 10% increase in frequency (as per Table 6).	Closed
T294	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-303]	Please specify for which use-cases (data, protocols) the throughput will be measured and has to increase by 10% year over year	The 10% increase is applicable to all protocols listed in Table 6.	Closed
T295	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-306]	Make optional or delete. This requirements exclude vendors that do not support authentication and authorization based on the RADIUS protocol as they have followed a different approach.		Pending
T296	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-116]	Suggestion to delete due to information security issues related to this feature or make optional		Pending
T297	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-121]	The IEG-C SHALL support the use of IPv6 without impaired functionality and performance within a network environment. > Many information assurance authorities / accreditation bodies do not consider IPv6 secure enough and thus do not allow it for relevant products. Suggestion to make IPv6 an optional feature supported once accepted by the relevant authorities	This is a requirement for the IEG-C. IPv6 should be supported (this doesn't necessarily mean certified)	Closed
T298	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-148]	Just randomly adding system resources to evaluated and approved Web Guard products that are part of the IEG-C solution is not allowed without prior approval from national or NATO information assurance authority. Suggestion to delete or make optional vertical scalability	SRS amended	AMD4
T299	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-147]	Web Guard - Requirement to "allow for multiple instances of the WG to be deployed on multiple machines" appears to favor single product and is directly associated with "*****" product deployment capabilities (Cloud, physical, virtual). Suggestion to delete or alter so that alternative solutions that meet the requirement of "horizontal scalability" can be proposed	SRS amended	AMD4
T300	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-152]	Requirement is too vague. Suggestion to delete or remove SHALL. What does learnability mean? How is it measured? Skills of the "system administrator" are unclear. Why can it not expected that a system administrator reads the manual or does prior training when dealing with a product supposed to protect NATO SECRET information?	SRS amended	AMD4
T301	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-157]	Web Guard - Limiting the maximum size of the audit log undermines core information assurance aspect of WG and requirements from national / NATO security authorities. The audit log is a key element for forensics related to classified information protection. Suggestion to delete		Pending
T302	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-239]	Mail Guard - Limiting the maximum size of the audit log undermines core information assurance aspect of MG and requirements from national / NATO security authorities. The audit log is a key element for forensics related to classified information protection. Suggestion to delete		Pending
T303	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-230]	Mail Guard - Requirement to "allow for multiple instances of the MG to be deployed on multiple machines" appears to favor single product and is directly associated with "*****" product deployment capabilities (Cloud, physical, virtual). Suggestion to delete or alter so that alternative solutions that meet the requirement of "horizontal scalability" can be proposed		Pending
T304	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-231]	Just randomly adding system resources to evaluated and approved Mail Guard products that are part of the IEG-C solution is not allowed without prior approval from national or NATO information assurance authority. Suggestion to delete or make optional vertical scalability		Pending
T305	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-275], [SRS-6-274]	Requirement for scheduled WG management and e.g. updates of certificates does not meet information assurance authority requirements for cross domain solution products tasked with protecting NATO SECRET information. Alternatively this requirement could favor single product. Suggestion to delete or make optional		Pending
T306	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-506]	Requirement appears to favor specific WG. Suggestion to delete, make optional or add that the functionality can also be provided by PAN-3260 firewall		Pending
T307	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-508]	Requirement appears to favor specific WG. Suggestion to delete, make optional or add that the functionality can also be provided by PAN-3260 firewall		Pending

T308	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-509]	Requirement appears to favor specific WG. Suggestion to delete, make optional or add that the functionality can also be provided by PAN-3260 firewall		Pending
T309	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-512]	Requirement appears to favor specific WG. Suggestion to delete, make optional or add that the functionality can also be provided by PAN-3260 firewall		Pending
T310	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-513]	Requirement appears to favor specific WG. Suggestion to delete, make optional or add that the functionality can also be provided by PAN-3260 firewall		Pending
T311	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-514]	Requirement appears to favor specific WG. Suggestion to delete, make optional or add that the functionality can also be provided by PAN-3260 firewall		Pending
T312	AMD3	SRS (Book II Part IV Annex A)	[SRS-6-52]	WG must offer IPv6 > Many information assurance authorities / accreditation bodies do not consider IPv6 secure enough and thus do not allow it for relevant products. Suggestion to make IPv6 an optional feature supported once accepted by the relevant authorities	See answer to T297.	Closed
T313	AMD3	SOW (Book II Part IV)	SOW-381	<p>The Contractor SHALL provide all training modules and courses required to enable all initially assigned Purchaser personnel to operate and maintain the system at Level 1, 2 and 3. The Contractor SHALL ensure all activities, milestones and actors associated with IEG-C System Training are guided by the Training Plan.</p> <p>Question: 1. Please confirm that all personnel to be trained does have the required level of previous training in order to understand training delivered e.g. System administrators are familiar with expected topics about how to admin such a system.</p>	Training pre-requisites are expected to be clearly de-fined by the Contractor as part of the TNA, and will be agreed by the Purchaser.	Closed
T314	AMD3	SOW (Book II Part IV)	SOW-382	<p>The Contractor SHALL design, develop and deliver minimum the following trainings;</p> <ul style="list-style-type: none"> • System operations training • System maintenance training • Guard administration training • Other administration trainings (e.g. SMC, Security) identified during TNA • Train the Trainer (TtT) trainings • Test Crew trainings • Transition Training (in each site). <p>Questions: 1. Regards TtT Training: Is such training required for every level of training e.g. System operations training, System Maintenance Training etc. or is this topic related to e.g. one instructor to be coached to become such TtT for all topics listed above. 2. Regards Test Crew trainings: Request to further specify such training request with regards to how many individuals belong to “a crew”. What are the individual requirements for each individual within this crew training e.g. a crew consists of 1 (one) Ad-min; 1 (One) System Operator etc. 3. Regards Transition training: Are fundamental technical basics at each site are equal in order to deliver the trained required or are there specifics to be considered in advance.</p>	<p>1. TtT is required for all training types.</p> <p>2. Test crew does not in-clude operators or adminis-trators. This group is the testing team as part of the project managing each testing activity. It will be maximum of 12 people attending to these sessions.</p> <p>3. Site transition training will be based on introducing the local support personnel to installed physical site configuration for Level 1 maintenance and support tasks only.</p>	Closed

T315	AMD3	SOW (Book II Part IV)	SOW-383	<p>The Contractor SHALL design, develop, deliver and maintain the following types of training:</p> <ul style="list-style-type: none"> • Classroom Training (for operators, system administrators, guard administrators, engineers) • On the Job Training (for operators, system administrators, guard administrators, engineers) • Computer Based Training (CBT) modules for self-paced individual learning, compatible with the NCIA Learning Management System (only for NU). <p>Questions:</p> <p>1. At times you speak about maintainers and here you speak about engineers see SOW-382 System maintenance training. Are both the same, just a different wording in regards to training?</p> <p>2. CBT training:</p> <p>Please specify technical details in order to be “compatible with NCIA Learning Management System”.</p>	<p>1. Maintenance will be performed partially by the administrators and engineers.</p> <p>2. Please read all the SOW requirements. The standard that needs to be followed is given in SOW-419.</p>	Closed
T316	AMD3	SOW (Book II Part IV)	SOW-384	<p>As part of the system implementation the Contractor SHALL provide on-site training to all support staff designated by the Site POC and on all tasks required to operate, maintain and recover the IEG-C System.</p> <p>Question:</p> <p>1. Please specify in detail the amount of personal to be trained on-site per site location or is this equal to SOW-382 requirement “Transition training (in each site)”.</p>	<p>Amount of personnel to be trained for operation and maintenance is given in SOW-385 and SOW-386. Site Transition Training is a separate training for local support personnel, and will be limited to one session.</p>	Closed
T317	AMD3	SOW (Book II Part IV)	SOW-385	<p>As part of the training process the Contractor SHALL provide the on-site training course (operators and administrators/maintainers) for a maximum number of two sessions in Mons for each type of training as outlined in [SOW-384], or another site designated by the Purchaser or an online course. The Contractor SHALL provide the Transition Training in each installation site both for operation and maintenance, as applicable.</p> <p>Questions:</p> <p>1. How long should a session be?</p> <p>2. Each type of training in SOW-384? There are three types of training requested not only two in SOW-384. Operate-Maintain-Recover.</p>	<p>1. It is the Contractor’s responsibility to develop the training courses and propose the duration under TNA for Purchaser approval.</p> <p>2. Test crew trainings should be provided before each test event in line with its purpose. Site transition training should be provided once in each site in line with its purpose.</p>	Closed
T318	AMD3	SOW (Book II Part IV)	SOW-389	<p>As part of the training process the Contractor SHALL provide Train the Trainer courses for a minimum of 5 instructors designated by the Purchaser.</p> <p>Question:</p> <p>1. 5 (five) instructor per site or in total? Please specify the total number of instructor to be trained.</p>	<p>5 in total</p>	Closed
T319	AMD3	SOW (Book II Part IV)	SOW-387	<p>The Contractor SHALL use the Training Needs Analysis (TNA) to refine the number of training sessions needed for each role.</p> <p>Question:</p> <p>1. Please specify in detail the requested roles as those roles vary at times within the document.</p>	<p>Generic roles are already provided in the SOW. However, as the requirements SOW-402 and SOW-403 clearly state, as part of the TNA Target Audience Analysis, it is the Contractor’s responsibility to finalize the roles in accordance with the Purchaser’s maintenance and support organization.</p>	Closed
T320	AMD3	SOW (Book II Part IV)	SOW-386	<p>The Contractor SHALL provide each training session for a maximum of 12 persons per session.</p> <p>Question:</p> <p>1. Is this limit of 12 persons also valid for the test crew training?</p> <p>2. If yes, does the test crew therefore consists of not more than a maximum of 12 persons?</p>	<p>Correct, yes to both.</p>	Closed

T321	AMD3	SOW (Book II Part IV)	6.6.1.1	<p>The Purchaser will provide the following basic facilities: room, power supply, tables, chairs, network It is standard EU sockets providing main power supply.</p> <p>connectivity.</p> <p>Question:</p> <p>1. The power supply in each site is 220-240V and 50-60herz or may that vary from site to site?</p>		Closed
T322	AMD3		Answers to CR: T162	<p>The answer to CR T162 is incomplete.</p> <p>Question:</p> <p>1. Could you please provide the complete answer?</p>	the answer to 162 is Yes and it was answered in CR T2 with IFB amendment 2.	Closed
T323	AMD3	SRS (Book II Part IV Annex A)	[SRS-5-327]	Are there any additional information/requirement regarding available DRS?		Pending
T324	AMD3	SOW (Book II Part IV)	[SOW-870]	Are there any additional information about Purchaser CMDB tools?	see T246 and T247	Closed
T325	AMD3	SRS (Book II Part IV Annex A)	[SRS-4-67]	<p>A comparable/improved alternative to switch S3048 could be the Dell S3148T plus additional rear bay with 2 x 1/10 GbE ports. Would NCIA accept this model? A comparable/improved alternative to switch Dell N1124-T-ON switch (which is End of Sales) could be the Dell S3124T Would NCIA accept this model</p>	Yes. See T263	Closed