**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 1 | **Scope of Work** S.no 4.a. in Annexure-I at page 1 of 4. | Review of Control Centre Architecture (NTAMC, BNTAMC, Electrical Region and Control Region) | What are the expected outcomes from this review? Is there any standard NTAMC considered for this review? | 1. Refer Sr.no 8 of "Terms & Condition…" in Annexure-III at page 1 of 2.<br>2. Refer Sr.no 4(e) of "Scope of Work", in Annexure-I at page 3 of 4. The standard & guidelines are mentioned there.<br>3. Finalized Architecture and network details shall be provided by POWERGRID during Audit. |
| 2 | **Scope of Work** S.no 4.a. in Annexure-I at page 1 of 4. | Review of Control Centre Architecture (NTAMC, BNTAMC, Electrical Region and Control Region) | What are the in scope networks to be covered as part of architecture review? | Refer Sr.no 1. |
| 3 | **Scope of Work** S.no 4.a. in Annexure-I at page 1 of 4. | Review of Control Centre Architecture (NTAMC, BNTAMC, Electrical Region and Control Region) | It is understood that Architecture diagrams of NTAMC, BNTAMC, Electrical Region and Control Region will be provided prior to the assessment. Please confirm. | Confirmed. |
| 4 | **Scope of Work** S.no 4.a. in Annexure-I at page 1 of 4. | Review of Control Centre Architecture (NTAMC, BNTAMC, Electrical Region and Control Region) | Approximately how many networks exist per site | Finalized Architecture and network details shall be provided by POWERGRID during Audit.<br>At least 35 networks at Main NTAMC, 35 networks at Back up NTAMC, 20 networks at ER-RTAMC and 8 networks at CR-RTAMC. |
| 5 | **Scope of Work** S.no 4.c. in Annexure-I at page 2 of 4. | Penetration Testing (Internal and External) | 1. Is VAPT to be conducted both from within the network and from outside, if yes: | 1. Yes, from Within Network and from outside.<br>a. Interfacing network devices. Refer Sr.no 4 for number of network details. |

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| | | | a. What are the systems to be covered under the external VA<br>b. How will access to these systems be provided, as annexure IV 1.4 specifically mentions that all the work shall be carried out at the premises | b. Through interfacing Network devices from Main NTAMC premise. |
| 6 | **Scope of Work** S.no 4.d.i in Annexure-I at page 3 of 4. | **Verification of CVE-ID and CVSS Scores:** The Technical Specification of NTAMC project consists of Inventory Management Software which shall be provided by contractor. It shall cover all software inventory, installation dates, CVE IDs along with CVSS scores for the applications that will be delivered. Vol-II, Part-B, Section-4, 4.7 (Software). | Please share the details related to Vol-II, Part-B, Section-4, 4.7 (Software). It is not available in this RFP. | 1. Type of Software items are mentioned in "Item Category" of "List" i.e Annexure II(b) and Annexure II(c).<br>2. The exact make/versions of software shall be provided during audit. |
| 7 | **Scope of Work** S.no 4.d.iii in Annexure-I at page 3 of 4. | **Verification of CVE-ID and CVSS Scores:** Contractor shall provide list of software for which CVE/CVSS scores are not published by OEM. Procedure to mitigate vulnerabilities in such system shall also be suggested by the contractor." | It is understood that Cyber security auditor has to review the vulnerability status of Software Asset Management software. Carrying out the Security testing of Software asset management solution is not part of scope of work. Please confirm. | Security testing is required for verifying the Policies, and configuration of various software and the networking devices. |
| 8 | **Scope of Work** S.no 4.d.iii in Annexure-I at page 3 of 4. | **Verification of CVE-ID and CVSS Scores** | How would the auditor obtain the inventory for the verification of CVE-ID and CVSS scores? | The exact make/versions of software shall be provided during audit.<br>Type of Software items are mentioned in "Item Category" of "List" i.e Annexure II(b) and Annexure II(c). |

**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 9 | **Scope of Work** S.no 4.e in Annexure-I at page 3 of 4. | **Review of Cyber Security Requirements:** The scope of audit shall include review "Cyber Security Requirements" in line with the following…….. | It is understood that Cyber security auditor has to review the cyber security requirements of equipment as per the Annexure V. Auditor will also perform the review related to cyber security of equipment based on NCIIPC, CEA, IEC 62443-3-2 and ISMS Policy. However, Compliance review to NCIIPC, CEA, IEC 62443-3-2 and ISMS Policy is not part of scope of work. Please confirm. | Confirmed that Compliance review is not under the scope of work of auditors.. |
| 10 | **Scope of Work** S.no 4.e in Annexure-I at page 3 of 4. | **Review of Cyber Security Requirements:** | What would be the scope of cyber security requirement review? Please share the in scope packages and systems in scope along with OEM? | 1. Bidder to comply scope of work.<br>2. Systems are mentioned in the BOQ . The OEM details shall be provided during the Audit. |
| 11 | **Scope of Work** S.no 4.e.iv in Annexure-I at page 3 of 4. | Risk Assessment as per IEC 62443-3-2 | Is a Risk Assessment as per IEC 62443-3-2 to be carried out? | Yes |
| 12 | **Scope of Work** S.no 5 in Annexure-I at page 3 of 4. | Any interfacing devices that are connected in Control Centre OT network for log transferring/collection to external agencies like NCIIPC, C-SOC etc. shall also be included in the scope of audit. | Where are these logs stored? Are they on a normal server or any other SACADA device? | The Interfaces devices for log transfer include 1 Server & 1 Router at Main NTAMC. |
| 13 | **Scope of Work** S.no 5 in Annexure-I at page 3 of 4. | Any interfacing devices that are connected in Control Centre OT network for log transferring/collection to external agencies like NCIIPC, C-SOC etc. shall also be included in the scope of audit. | Could you please highlight what devices are to be covered? | Refer Above Sr.no 12. |

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 14 | **Scope of Work** S.no 6 in Annexure-I at page 3 of 4. | Typical Network devices viz. Router cum Firewall, Switches at substations which are dedicatedly integrated in the network with the NTAMC Control Centre shall also be included in the scope of audit on sample basis. | 1. How many substations are connected with each control centre?<br>2. If auditing at separate locations is necessary, please provide the list of locations and respective BoQs included in the audit (Cyber Security BoQ during SAT).<br>3. What is the sample size? Will samples be chosen control centre-wise or substation-wise?<br>4. Will auditor access to regional centre devices be allowed remotely, or must the auditor visit each site physically? Is the auditor's connectivity through MPLS or another medium? | 1. On sample basis, 02 S/s per control centre i.e total 26 S/s shall be considered. 01 S/s is having 02 Router cum Firewall, 04 Switches, 01 Network Video Recorder, 03 PCs, Jump Server & VoiP Phone.<br>2. Audit of S/s devices & other control centres to be done centrally from Main Control Centre (Manesar) during SAT. The quantity of devices/items in respective control centres is mentioned in Annexure-II.c. to be read as follows:<br>A. Main Control Centre is Main NTAMC at Manesar i.e from sr.no 1 to 71 of Annexure-II.c.<br>B. Back up Control Centre is Back up NTAMC at Banglore i.e from sr.no 71 to 136 of Annexure-II.c.<br>C. **Client Regional Control Centres** (06 Nos) list of items for:<br>i. NR-1 RTAMC (Manesar): Sr.no 137 to 155 in Annexure-II.c.<br>ii. NR-2 RTAMC (Lucknow): Sr.no 156 to 174 in Annexure-II.c.<br>iii. ER-1 RTAMC (Patna): Sr.no 214 to 232 in Annexure-II.c.<br>iv. Odisha RTAMC (Bhubaneshwar): Sr.no 272 to Sr.no 290 in Annexure.II.c.<br>v. SR-2 RTAMC(Banglore): Sr.no 369 to Sr.no 387 in Annexure.II.c. |

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| | | | | vi. WR-1 RTAMC (Nagpur): Sr.no 388 to Sr.no 406 in Annexure.II.c.<br>D. **Electrical Regional Control Centres** (5Nos) list of items for:<br>i. NR-3 RTAMC (Lucknow): Sr.no 175 to 213 in Annexure-II.c.<br>ii. ER-2 RTAMC (Kolkatta): Sr.no 233 to 271 in Annexure-II.c.<br>iii. NER RTAMC (Guwahati): Sr.no 291 to 329 in Annexure-II.c.<br>iv. SR-1 RTAMC (Hyderabad): Sr.no 330 to Sr.no 368 in Annexure.II.c.<br>v. WR-2 RTAMC (Vadodra): Sr.no 407 to Sr.no 445 in Annexure.II.c.<br>3. Refer above point 1.<br>4. Auditor access to other control centres shall be provided remotely from Main Control Centre (Manesar) through MPLS. |
| 15 | **Scope of Work** S.no 6 in Annexure-I at page 3 of 4. | Typical Network devices viz. Router cum Firewall, Switches at substations which are dedicatedly integrated in the network with the NTAMC Control Centre shall also be included in the scope of audit on sample basis. | Could you please highlight the in scope devices (approx.) that would be covered as part of the audit ? | Refer above Sr.no 14 |
| 16 | Annexure-II.c | Control Centre Software list from Sr.no 47 to 71. | FAT and SAT BoQ item Clarification (Annexure-IIa scope of work):<br><br>1. From items 47 to 71 in SAT BoQ, we can audit the implementation as per NTAMC policy for standard software like antivirus, etc., unless the source | The standard software shall also be checked for missing security updates and configuration issues in the audit. |

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| | | | code is available; however, VAPT cannot be conducted. We may only check the license and count of installations.<br>2. As per the standard audit scope, items listed in FAT and SAT BoQ such as Standard MS Office software, Monitors (without network interface), voice recorders (without network interface), Standard Antivirus Software, EDR, and SACDA standard software are out of the scope of audit work. If specific audits for these items are required, please suggest. | |
| 17 | **Bill of Quantity** (Annexure-IIa) | Cyber Security Audit SCAN & Re-SCAN of setup made with all Hardware and software associated with Main Control Center, Backup Control Center, 5 x Regional Control Centers and 6 x Client Control Centres as per the list enclosed at Annexure-II(c) during SAT. | 1. It is understood from the List of Hardware and Software as per Annexure-II(c) that mentioned list is total inclusive of 5 Electrical regional centres equipment and 6 Client Regional control centers respectively. Please confirm.<br>2. If the list is only for one regional control center, then to get the total hardware and software ,can we multiply by 5 ? Please confirm. | 1. Confirmed.<br>2. Refer above Sr.no 14. |
| 18 | **Bill of Quantity** (Annexure-IIa) | | Who will be selecting the sites that are to be audited - PGCIL or the Auditor ? | All Control Centres are to be audited during SAT i.e. total 13 nos.<br>For Substations: Refer clarification above in Sr.no 14 including sample size of S/s. Location of S/s shall be decided during audit by POWERGRID. |

**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 19 | (Annexure-IIb) List of Hardware for Cyber Security Audit during FAT: | CONTROL CENTRE-SOFTWARE (Sr.No: 38 to 61), (Sr.No: 99 to 122) (Sr.No: 144 to 153) (Sr.No: 165 to 169) | Kindly provide the below details for estimation,<br>1. Approx. no of dynamic pages<br>2. Type of application: Desktop/Web application<br>3. Name of Hosted web applications.<br>4. Application is part of management Software? (Eg. Switch/Router Management Console, Firewall Management).<br>5. Please provide the inputs related software application in the 'input form' attached for each application.<br>6. It is suggested not perform the application security testing on the Switch/Router/Firewall/Antivirus/HIDS/SIEM Management console. However platform and configuration releated vulnerabilites will be reviewd as part of scope of work. Please confirm. | - Sr.no 1 to 5: Query of Details/Inputs shall be taken up during audit, if required. Bidder to comply scope of work.<br>- Sr.no 6: The standard Hardware/software shall also be checked for missing security updates and configuration issues in the audit. |
| 20 | (Annexure-IIb) List of Hardware for Cyber Security Audit during FAT: | List of Hardware for Cyber Security Audit during FAT: | Computer System Hardware-E-Mail Server :<br><br>1. Is the email server in the OT network<br>2. If no, are system in the IT network in scope | 1. Yes.<br>2. Systems in the IT network not in scope. |
| 21 | (Annexure-IIb) List of Hardware for Cyber Security Audit during FAT: | Sr.no 123 – MS Office Software | MS office Software - Which applications are present? | Complete MS Office Suite |

**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 22 | (Annexure-IIc) List of Hardware for Cyber Security Audit during SAT | CONTROL CENTRE-SOFTWARE (Sr.No: 47 to 70), (Sr.No: 112 to 135) (Sr.No: 144 to 150, 168, 199 to 208, 226, 257 to 266, 284, 315 to 324, 354 to 363, 381, 400, 431to 440, to ) (Sr.No: 165 to 169) | Kindly provide the below details for estimation,<br>1. Approx. no of dynamic pages<br>2. Type of application: Desktop/Web application<br>3. Name of Hosted web applications.<br>4. Application is part of management Software? (Eg. Switch/Router Management Console, Firewall Management).<br>5. Please provide the input related software application in the 'input form' attached for each application.<br>6. It is suggested not perform the application security testing on the Switch/Router/Firewall/Antivirus /HIDS/SIEM Management console. However platform and configuration related vulnerabilities will be reviewed as part of scope of work. Please confirm. | Refer above clarification at Sr.no 19. |
| 23 | **Bill of Quantity** (Annexure-II.b & II.c) List of Hardware for Cyber Security Audit | Control Centre Software Items in List | Please confirm that the software application used in Main Control Center, Backup Control Center, 5 x Regional Control Centers and 6 x Client Control Centres are same?. Is there any difference in functionality or usage? Please provide us details. | 1. Software at Main & Back up Control Centre are same.<br>2. Few Software at Electrical & Client RTAMC are subset of Main Control Centre Software.<br>3. The exact make/versions of software shall be provided during audit. |

**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 24 | **Terms & Condition……** S.no 5 in Annexure-III at page 1 of 2. | The laptop, honeypot or any device once set for carrying out the audit shall not be carried outside of NTAMC premises during the entire period of audit, till completion of the audit. | Are the systems used for testing not allowed to be taken out even after completion of individual activities like scan phase (initial testing) | Allowed, after completion of individual activities like scan phase (initial testing) |
| 25 | **Terms & Condition……** S.no11 in Annexure-III at page 1 of 2. | Scanning should cover all aspects of the devices including the operating system, web server, application code, and third-party libraries. | 1. It is understood that Source code review of application software(s) are not part of scope of work. Please confirm.<br>2. If Source code review has to be performed. Kindly provide the details of application.<br>3. Is the supplier(s) of the software application providing any undertaking about the security posture / security audit reports/ source code review report from their end, and if so can those be made used for souce code review?. Please clarify. | 1. Confirmed.<br>2. Source code review is not required<br>3. No, such documents are not available from the supplier. |
| 26 | **Terms & Condition……** S.no11 in Annexure-III at page 1 of 2. | Scanning should cover all aspects of the devices including the operating system, web server, application code, and third-party libraries. | Can scripts/custom tools be used to perform certain activities, eg - OS hardening assessment | Yes |
| 27 | **Terms of Reference** S.no 2 in Annexure-IV at page 1 of 1. | Timelines for deliverables: | Is the timeline for completion of the audits during FAT and SAT (1 month and 3 months) applicable per site of for all sites combined | 1. During FAT - Applicable for all control centres as mentioned in Annexure II.b.<br>2. During SAT - Applicable for all control centres as mentioned in Annexure II.c.<br>. |

**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

<table>
<tr><th>Sr.no</th><th>Clause</th><th>Provision of Bidding Documents</th><th>Bidder's Query</th><th>POWERGRID's Reply</th></tr>
<tr><td>28</td><td>Terms of Reference<br>S.no 2 (c) in Annexure-IV at page 1 of 1.</td><td>The initial scan and re-scan during FAT or SAT may not be carried out in one visit and may require to make multiple visits.</td><td>1. How many such rounds of FAT / SAT activities and associated audits are expected during the 1.5 years of contract. Please clarify.<br>2. We assume that one visit for Initial scan and after remedial action one more visit for re-scan. It means that all the reported vulnerabilities will be fixed during re-scan. Please confirm</td><td>1.(i) FAT (Factory Acceptance Test) is one time activity. The complete Set-up of FAT system shall be done at L&T works in NOIDA where FAT is to be done. The list of items covered in audit during FAT is mentioned in Annexure II b.<br>1(ii) SAT (Site Acceptance Test) is also one time activity for each control centre. Also, refer clarification at Sr.no 14.<br><br>2 Yes, as per audit of FAT and each SAT activity.</td></tr>
<tr><td>29</td><td>Terms of Reference<br>S.no 2 (b) in Annexure-IV at page 1 of 1.</td><td>An advance intimation, generally one week ahead of the scheduled date of the initial &<br>re-scan audit shall be given. Agency must deploy Auditor within one week of intimation.<br>The auditing timelines for FAT & SAT Shall be as given below:<br>FAT (Audit Completion Schedule):<table><tr><th>Initial Audit</th><th>Re-Scan Audit</th></tr><tr><td>1 Month</td><td></td></tr></table></td><td>Timeline of project: 2(b), Annexure-IV – Scope of work: Clarification is needed on the timeline for initial audit and re-scan audit. Is the duration of 1 month for each audit work or total for both? If it is 1 month each, it seems insufficient, as a minimum of 2 to 3 months is required for complete FAT audit work.</td><td>Duration of 01 Month is applicable including initial & Re-Scan time. Provided, the employer fixes the vulnerabilities & offers the system for rescan.<br>Multiple teams to be deployed, if required.</td></tr>
<tr><td>30</td><td>Cyber Security Requirements<br>S.no 9.3.1 in Annexure-V at page 6 of 19.</td><td>……scripts shall be provided to help harden the operating system……</td><td>It is understood that performing mitigation actions are not part of scope of work. Please confirm.</td><td>Yes. However, procedures to mitigate vulnerabilities to be suggested.</td></tr>
</table>

**Clarification - I to Bidding Documents for Package Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT; Gem Bid No.: GEM/2024/B/5151558**

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| 31 | **Cyber Security Requirements** Annexure-V | Cyber Security Requirements<br><br>(Technical Specifications of Upgradation of SCADA and Associated Systems of NTAMC/RTAMC) | As per our understanding this section is the technical specification of Upgradation of SCADA system and the scope of this tender will be limited to the Audit of the mentioned system. | The scope of this tender is limited to the Audit of the mentioned system in the BoQ.<br><br>This Technical Specification is to be used as reference according to which the Cyber Security implementation of the System is to be reviewed. |
| 32 | General | - | Is the NTAMC in airgap? Also, for auditing at the NTAMC premises, are auditor laptops allowed? | Yes. NTAMC is airgap.<br>,As per ISMS & BYOD policy which shall be shared after award. |
| 33 | General | - | Audit location Query: For audit locations other than those mentioned in the SAT and FAT BoQs (i.e., Noida and Manesar), travel, stay, and other charges will be paid by the client. | 1. Refer "Note:" mentioned in Annexure-II(a). Also, refer clarification above at Sr.no 14.<br>2. Bidder to comply scope of work. |
| 34 | General | - | What is the approximate duration between the initial scan and revalidation scan expected to be ? | Refer Sr.no 2 of Terms of Reference i.e Annexure- IV. Provided, the employer fixes the vulnerabilities & offer the system for rescan. |
| 35 | Annexure – X to Section-III<br><br>Qualification Requirement of the bidder for Cyber Security Audit of | The bidder is a Government Auditor | Please refer to the Technical Experience at page 40 in the ATC Tender Document, It is mentioned that "the bidder must be a Government Auditor" and audit must will be done with NCIIPC Guidelines.<br><br>We have gone through the SOP of NCIIPC, There is a confusion at two places in this | The bidder must be a Government Auditor.<br><br>"Government Auditor" means Government Organization / Government Agency. |

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| | SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT | | SOP, as at Point Number 6.2.1.2, it is mentioned that Cyber security audit of a "Critical Segment Category-I" must be carried out by a Government auditor, while at Point Number 7.1. it is mentioned that Private/Government Auditors will be selected for auditing CII/Protected Systems (including Critical Segment Category-I and Critical Segment Category-II). | Bidder to Comply "Qualification Requirement" as per "Annexure – X to Section-III (Qualification Requirement of the bidder for Cyber Security Audit of SCADA and associated Systems of NTAMC Upgrade Project during FAT and SAT)". |
| 36 | **Qualification Requirements** S.no 2.1 in Annexure-X of Section-III | **TECHNICAL EXPERIENCE** The bidder must be a Government Auditor. | Kindly clarify what is the definition of a "Government Auditor" for the purpose of this bid, and can "XXX" considered as an Auditor as our organization is working with multiple government entity on similar engagements? | Bidder to comply Qualification Requirement also refer Sl. No 34 above |
| 37 | **Qualification Requirements** S.no 2 in Annexure-X of Section-III | **TECHNICAL EXPERIENCE** | As part of our technical experience, our organization is CERT-In and MeitY empaneled. In light of this, I would kindly request clarification on whether we are eligible to participate in the bid under consideration. | Bidder to comply Qualification Requirement. |
| 38 | 6.1.2, Section-III, conditions of contracts | The proposal security shall, at the bidder's option, be in the form of a crossed bank draft/pay order /banker certified cheque in favour of Employer i.e. 'Power Grid Corporation of India Limited' payable at Delhi/Gurgaon or a bank guarantee from a reputed bank or Insurance Surety Bond from an Insurer as per guidelines issued by Insurance Regulatory and Development Authority of India (IRDAI) selected by the bidder. The format of bank guarantee/ Insurance | Please provide the Beneficiary details for EMD and EMD validity details | Bidders are requested to refer Clause no 6.1.2 of Section-III, conditions of contracts in Buyer Specific Additional Terms and conditions which are amply clear |

| Sr.no | Clause | Provision of Bidding Documents | Bidder's Query | POWERGRID's Reply |
|---|---|---|---|---|
| | | Surety Bond shall be in accordance with the form of proposal Security included in the RfP documents, Proposal Security shall be valid up to **05/04/2025** or any other date as subsequently requested under clause 2.3.2 above. | | |