To
The Executive Directors/Directors/Director-in-charge
All NIELIT Centres

Sub: Personnel Policy for Group ‘A’ S&T Officers of Ministry of Electronics and Information Technology (Meity) and its organizations – Instructions for Autonomous Bodies – regarding

Sir/Madam,

A letter No.1(03)/2016-NIELIT (Pt.II)/113 dated 18th January, 2017 was forwarded/circulated to All NIELIT Centres including Group ‘A’ S&T Officers of NIELIT Headquarters, in which, it was advised that the Annual Work Report format, Part-A contains the self appraisal report which will be assessed by the Reporting Officer in Part-B of the Annual Work Report. The reporting officer while evaluating the self appraisal report shall give appropriate numerical grading from any of the Sub-categories of the product links filled by the officer reported upon for review promotion under the policy. The Reporting Officer shall also ensure that the numerical grading is accorded as per provisions of Annexure-II of the Meity Policy.

2. An Annual Work Report (AWR), has been designed to capture scientific content of work performed, would be filled up (only part A) by all S&T Officers alongwith the Annual Performance Appraisal Report (APAR) and would get reported upon by the Reporting Officer. The assessment of Screening Committee would be in part C of the AWR at the time of consideration for promotion under Personnel Policy.

3. NIELIT Headquarters are receiving the APARs dossiers of Group ‘A’ S&T Officers from NIELIT Centres for considering promotion to next higher grade, while scrutiny of the APARs dossiers of the S&T Officers, it has been found that Annual Work Report (Part A) has not filled up by the S&T Officers properly. Similarly, the Reporting Officer has also not assessed the Annual Work Report of the officer reported upon in Part-B. It is pertinent to mention here that Annual Work Report (Part A) and Part-B are essential for considering promotion of Group ‘A’ S&T Officers.

4. In view of the above, all NIELIT Centres, are, therefore, requested to check the APARs dossiers properly, while forwarding the cases of Group ‘A’ S&T Officers for considering promotion. Incomplete documents i.e. non availability of APARs (as per residency period), Annual Work Report etc. will not be accepted by Headquarters.

Thanking you,

Yours faithfully,

[Signature]

Registrar

---

An Autonomous Society under Ministry of Electronics and Information Technology
NIELIT Bhawan, Plot No. 3, PSP Pocket, Institutional Area, Sector-8, Dwaarka, New Delhi-110 077
NIELIT Bhawan, Plot No. 3, PSP Pocket, Institutional Area, Sector-8, Dwaarka, New Delhi-110 077

Website - www.nielit.gov.in
Ref. No. 1(16)/2016-NIELIT/157

15th May, 2017

To
The Executive Directors/Directors/Director-in-charge
All NIELIT Centres

Sub: Frequently Asked Questions (FAQ) on Annual Work Reports- Regarding

Sir/Madam,

New Promotion Policy has been introduced by MeitY for all Group ‘A’ S&T Officers and its organizations, vide OM No. 2(11)/2016-Pers-III dated 19/09/2016, termed as “New Personnel Policy for Group ‘A’ S&T Officers”

3. Under this Personnel Policy, the quantified S&T output indicators are provided in the Annexure of the AWR format. The reporting officer while evaluating the self appraisal report shall give appropriate numerical grading from any of the Sub-Categories of the Product Links filled by the officer reported upon for review promotion under this policy. The Reporting Officer shall also ensure that the numerical grading is accorded as per provisions of MeitY’s policy. The candidate requires to obtain minimum 20 marks per assessment year from any of the sub-categories from any of the product links for review under this policy.

4. Regarding criteria for output indicators and numerical grading from any of the sub-categories of the product links filled by the officer reported upon for review promotion under the policy as mentioned at para 6, NIELIT has received clarification from ABC Division, MeitY vide their letter No. 14(2)/2016-ABCD dated 10th January, 2017, wherein it has been stated that as per practice adopted in MeitY, to assess the candidates as per the old AWR format in case the AWRs have already been submitted/completed. However, fresh AWRs (i.e. Year 2015) shall be evaluated as per the provisions of the existing policy of MeitY.

5. In view of the above, a communication received vide letter No. 14(2)/2016 dated 9th May, 2017) from ABC Division, MeitY alongwith a Frequently Asked Question (FAQ) on Annual Work Report vide O.M. No. 2(11)/2012-P.III dated 05.05.2017 (copy enclosed) is sent herewith to NIELIT Centres to comply with these guidelines as mentioned in the aforesaid communication.

Thanking you,

Yours faithfully,

(Finan Raij)
Registrar

CC: IT Wing - for upload the communication on NIELIT Website in Employees Corner

An Autonomous Society under Ministry of Electronics and Information Technology
To

Director General
NIELIT

Subject: Frequently Asked Questions (FAQ) on AWRs – reg.

Sir/Madam,

Please find enclosed a copy of communication No. 2(11)/2012-P-III dated 05.05.2017 received from Personnel-III Section of this Ministry on the above subject for information and compliance.

Encl: As above

Yours faithfully,

[V. Rajalakshmi]
Section Officer
Tel: 24301793

Registrar's Office
Diary No. 11/5
Date In. 11/5
Date Out. 11/5

DG, NIELIT

Digital India
Subject: Frequently Asked Questions (FAQ) on AWRs.

With regard to the above mentioned subject, several representations/doubts were received from by Group 'A' S&T officers of MeitY, which have been examined and clarifications in the form of Frequently Ask Questions (FAQ) are given in the table below:

<table>
<thead>
<tr>
<th>Sl.</th>
<th>Point of Doubt</th>
<th>Clarification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Whether AWR is submitted once for whole residency period OR annually?</td>
<td>AWR is to be submitted annually as decided vide MeitY’s communication No. 2(11)/2012-P.III dated 07.03.2013.</td>
</tr>
<tr>
<td>2.</td>
<td>Timeline for submission of AWRs.</td>
<td>The instructions on timeline applicable to ACRs/APARs will be complied for AWR also. Timeline for submission of APARs in MeitY has been notified vide MeitY’s O.M. No. 7(2)/2012-P.III dated 28.01.2015.</td>
</tr>
<tr>
<td>3.</td>
<td>How all the subcategories in MeitY’s Policy will be linked to points specified in Annexure to AWR?</td>
<td>“Annexure to the AWR” has provisions for recording ‘Output Indicators’. In case any sub-categories provided in the ‘Output Indicators’ could not be recorded in the Annexure to AWR, a separate sheet, duly signed by the officer reported upon shall be added.</td>
</tr>
<tr>
<td>4.</td>
<td>Clarification on 5 Marks in Output Criteria on the following:-</td>
<td>As per the extant policy, a candidate is required to secure at least 20 marks in each year from any of the sub-categories (5 marks each) of any of the Product Links for review promotion.</td>
</tr>
<tr>
<td></td>
<td>i. Partial fulfillment/ exceeding the indicated criteria.</td>
<td>In order to obtain full 5 marks from each sub-category of a Product Link, a candidate has to achieve certain number of units i.e., 01 or more than 01 unit in each the Output Indicator.</td>
</tr>
<tr>
<td></td>
<td>ii. Marks for acquiring Master's degree</td>
<td>In the case of those sub-categories of output indicators/Product Link requiring 01 unit, proportionate marks will not be allowed for partial fulfillment. 5 marks will be given to those who fulfil the required 01 unit.</td>
</tr>
<tr>
<td></td>
<td>iii. Whether the point for acquiring Ph.D/previous work experience will be counted only in 1 year or for each year.</td>
<td>However, for those sub-categories of Product Link requiring more than 04 unit, proportionate marks out of 05 marks will be allotted.</td>
</tr>
<tr>
<td></td>
<td>iv. Benchmark for claiming marks</td>
<td>As regards acquiring Ph.D/Masters degree, a candidate will be required the best fit.</td>
</tr>
</tbody>
</table>
design know-how / technical initiatives.


5. Elaboration of the scope of each sub-category with suitable example(s).

Mr. 'X' gets minimum 20 marks, 5 marks each from the prescribed sub-category.

But, Mr. 'Y' gets 50 marks, 5 marks each sub-category from the 16 Product Links.

Since the minimum eligibility for promotion to the next higher grade is 20 marks under the policy, both Mr. X & Y are eligible for promotion. Further, as ranking/numerical grading system is not in vogue in the review promotion, the concept of higher/less priority for Mr. 'X' & 'Y' (based on the 20 & 50 marks obtained in AWRs) and seniority does not exist.

The eligibility of Mr. 'X' & 'Y' for promotion to the next higher grade will be considered subject to their performance before the DPCs/Assessment Board.

6. Difficulty of fulfilment of criteria for Output Indicators in some of the sub-categories in one year.

The policy has been designed to fulfill the requirement of MeitY and its organizations. Further, 'Output Indicators' have been extended to the maximum to ensure that, the work performs in MeitY by all S&T officers are covered by the policy.

The concept of, "the assessment process shall be rigorous with due emphasis on evaluation of scientific and technical knowledge so that only those scientists who have their credit demonstrable achievements or higher level of technical merit, are recommended for promotion" as laid down in the policy shall prevail. Every candidate, who fulfills the minimum eligibility and who have to their credit demonstrable achievements or higher level of technical merit before the DPCs/Assessment Board only are fit for promotion under the extant policy.

Group 'A' S&T officers, who are unable to fulfill the minimum eligibility and credit demonstrable achievements or higher level of technical merit before the Assessment Board/DPC, are not fit for recommendation for promotion under the extant policy.

7. Each scientific officer has to submit APAR each year. It was observed that the work details brought in APAR is mostly replicated in AWR since both

The principal objective of Annual Performance Appraisal Report (APAR) is to improve the performance of the subordinate in his present job and also to assess his potentialities and provide him appropriate feedback and guidance for correcting his deficiencies and improve his performance. APAR provides basic and vital inputs for assessing the performance of an officer.
which forms the basis for evaluating the merit of the concerned S&T officers.

The reporting/reviewing officer assessed the overall performance of the officer such as work output, personal attributes, functional competency etc., in the APAR. Hence, unlike AWR, the scientific content of the work done by the scientist could not be reflected in the APAR.

8. **Explanation on Field experience for promotion to Sci. 'F' (2 yrs) and Sci. 'G' (5 yrs)**

Every scientist who is eligible for consideration for promotion to the grade of Sci. 'F' and Sci. 'G' shall provide the details of field experience in additional sheet for the entire residency period.

2. Besides, a sample of Self Appraisal Report format for writing the AWR in accordance with the Personnel Policy of MeitY is also enclosed herewith for ready reference.

Encl: As above.

To,

(i) All GCs for kind information.
(ii) DD(Pers.) / DD (ABCD)

Copy to,

(i) IntraMeitY.
Annual Work Report (........ to ........)

Part IV

SELF ASSESSMENT BY THE OFFICER REPORTED UPON

1. Name: ........
2. Designation: ........
3. Area of S&T function:
   a) System administration
   b) Incident handling
   c) Mail administration
   d) Administration of Firewall
   e) Intrusion Prevention System administration
   f) Administration of Anti Virus Gateway Servers for domain users and DMZ
   g) Administration of WSUS
   h) Administration of Domain Controller
   i) Log analysis
   j) Installation of Tools/Software/Systems
   k) Participation in all the National/International Incident Handling and cyber security Drills conducted and participated by CERT-In/CERTs across the world.

4. Brief Description of S&T work function:

System Administration functions:
   b) Computer Security Incident Handling.
   c) Installation of update, security patches and service packs as and when needed to keep the network up to date and safe from outside and inside threats.
   d) System administration of Mail servers.
   e) Administration of Firewall
   f) WSUS administration
   g) Intrusion Prevention System administration: - Intrusion prevention mechanism was configured for protecting CERT-In infrastructure safe from cyber threats.

Log analysis :-
   * Logs of all the servers & security devices analyzed on daily basis. At the time of analysis malicious log entries separated out. As per the malicious logs corrective measures applied.

Installation/updating of Tools/Software System :-
   a) Packet analyzer Tools
   b) Network monitoring Tools
   c) Vulnerability scanners & Penetration Testing Tools.
   d) Encryption software
   e) Antivirus/Anti-malware software
   f) Operating System, Application Software installation/update/upgrade

National/International Incident Handling and Cyber Security Drills :-
   * Participated in all the National/International Incident Handling and cyber security Drills conducted and participated by CERT-In/CERTs across the world.
<table>
<thead>
<tr>
<th>SI No</th>
<th>Product Link</th>
<th>Sub Category</th>
<th>Details</th>
</tr>
</thead>
</table>
| 1     | M. ICT                       | Operations, Management and Maintenance in Office                              | 1) Customization of the network as per the CERT-In's needs, such as adding/update/upgrade software and hardware for smooth efficient and secure operation of computer network.  
     | Infrastructure Product Links  |                                                                               | 2) Performance monitoring.  
     |                                |                                                                               | 3) Troubleshooting, logging errors, assigning permissions to users.  
     |                                |                                                                               | 4) Backing up and restoring data.  
     |                                |                                                                               | 5) Security Incident/ threats related to CERT-In infrastructure analysed and resolved successfully. |
| 2     | D. S&T Management Product Link| Technical support                                                             | 1) Installing and configuring system hardware and software.  
     |                                |                                                                               | 2) Establishing and managing user accounts, assigning permissions to users.  
     |                                |                                                                               | 3) Installing and updating/patching system software.  
     |                                |                                                                               | 4) Preventing the spread of viruses and malicious programs.  
     |                                |                                                                               | 5) Allocating mass storage space,  
     |                                |                                                                               | 6) System security management, creating a backup and recovery policy, performance monitoring.  
     |                                |                                                                               | 7) Helping internal and external users with their technical issues (Hardware as well as software). |
| 3     | M. ICT                       | Management and prevention of security threats/ vulnerabilities in Cyber Space   | 1) Logs of all the servers and security devices analysed on daily basis. New attacks identified.  
     | Infrastructure Product Link    |                                                                               | 2) Corrective and Prevention methods applied by modification in policies, updates, patches and service packs. |
| 4     | E. S&T Services Product Link  | Assembly/integration/testing                                                   | 1) Assembling/integration/testing of Software and Hardware procured based on the reports to add/update/upgrade  
     |                                |                                                                               | 2) Assembling/integration/testing of Software and Hardware procured for CERT-In users |
| 5     | E. S&T Services Product Link  | S&T information services – Analysis                                            | 1) Logs of Mail server - 1  
     |                                |                                                                               | 2) Logs of Mail server - 2  
     |                                |                                                                               | 3) Logs of Domain Controller  
     |                                |                                                                               | 4) Logs of Firewall - 1  
     |                                |                                                                               | 5) Logs of Firewall - 2  
     |                                |                                                                               | 6) Logs of Web server - 1  
     |                                |                                                                               | 7) Logs of Web server - 2  
     |                                |                                                                               | 8) Logs of mail Gateway 1  
     |                                |                                                                               | 9) Logs of mail Gateway 2  

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Product Link</th>
<th>Sub Category</th>
<th>Min. Units Required</th>
<th>Units Obtained</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>L. ICT Services Product Link</td>
<td>Capacity Building programme</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 7     | B. Technology Product Link | Process Know How | 1. Studied each and every process of securing OS and application software.  
2. Studied how to secure network and systems from newly detected viruses and malicious software. |  | |
| 8     | I. S&T Cooperation Product Link | National Competitiveness | Participated in all the International Incident Handling and cyber security Drills conducted and participated by CERT-In/CERTs across the world. |  | |
| 9.    | P. S&T Human Resource Product Link | Master's level education | M.Sc (IT) |  | |
| 10    | O. Career Product Links | Acquiring technical work experience before induction of DeitY in electronics and IT industry. (atleast 1 year) | ET&T an organisation of DeitY (14 Year) Private electronics Industry (2 Year) |  | |
| 11    | P. S&T Human Resource Product Link | S&T management courses | 1) Foundation Certificate in IT Service Management  
2) Direct Trainer Skills |  | |
| 12    | P. S&T Human Resource Product Link | Training on advanced technical and Analytical methodologies | 1) Master Trainers Programme  
2) Computer Forensics for Technical Staff  
3) Fundamentals of Incident Handling  
4) Information Security for Technical Staff |  | |

6. Enumeration of major outputs from S&T Function

<table>
<thead>
<tr>
<th>SI No</th>
<th>Product Link</th>
<th>Sub Category</th>
<th>Min. Units Required</th>
<th>Units Obtained</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>M. ICT Infrastructure Product Links</td>
<td>Operations, Management and Maintenance in Office</td>
<td>1</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>D. S&amp;T Management Product Link</td>
<td>Technical support – internal and external</td>
<td>5</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>M. ICT Infrastructure Product Links</td>
<td>Management and prevention of security threats/ vulnerabilities in Cyber Space</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>E. S&amp;T Services Product Link</td>
<td>Assembly/integration/testing</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>E. S&amp;T Services Product Link</td>
<td>S&amp;T information services – Analysis</td>
<td>10</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>L. ICT Services Product Link</td>
<td>Capacity Building programme</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>B. Technology Product Link</td>
<td>Process Know How</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>#</td>
<td>Resource/Link</td>
<td>Description</td>
<td>Score 1</td>
<td>Score 2</td>
<td>Score 3</td>
</tr>
<tr>
<td>---</td>
<td>--------------</td>
<td>-------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>8</td>
<td>I. S&amp;T Cooperation Product Links</td>
<td>National Competitiveness</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>F. S&amp;T Human Resource Product Link</td>
<td>Master’s level education</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>O. Career Product Links</td>
<td>Acquiring technical work experience before induction of DeitY in electronics and IT Industry, (atleast 1 year)</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>F. S&amp;T Human Resource Product Link</td>
<td>Foundation Certificate in IT Service Management</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>12</td>
<td>F. S&amp;T Human Resource Product Link</td>
<td>Training on advanced technical and Analytical methodologies</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

7. Innovation content of work done (about 100 words)

Computer Security Incident Handling:- Security Incident related to CERT-In infrastructure analysed, handled and resolved successfully. Handled cyber threats against CERT-In efficiently. New attacks identified at Anti Virus Gateway level, customised policy Prevention mechanism was developed.

Sun Cluster configuration is used for load balancer and failover facilities.
The data communication between server and storage took place through ether card. The problem of bottleneck was resolved by creating ether channel.
Vulnerabilities identified and patched in Solaris Operating Systems, servers, security devices and nodes. Upgradation of DNS server (H/W and S/W).

8. Major impact reported during the financial year (if any) for work done during previous three years.

- More secured and redundant IT services with high availability.
- System administration work of previous years was helpful in configuration of Network, Servers, security devices, IT infrastructure and associated electronic & electrical devices.
- System Administration experience was helpful in updating network and troubleshooting the problems.
- MTTR (Mean Time to Recover) of system was reduced. MTBF (Mean Time between failure increased. Due to aforesaid parameter our IT-Infrastructure was almost 365x24x7 as desired by CERT-In Emergency services.
- Security implemented patching up vulnerabilities identified by different tools such as Nessus, Nmap, Saint.
- Several new attacks identified before it may penetrates to our network.
- Helped other government organization in Inspection and testing of computer hardware.
- Cyber attacks reduced on CERT-In infrastructure by utilizing multiple ISPs and building good relationship with ISPs.
- Cyber attacks reduced by implementing firewalls, IPSs and virus gateways.
- Daily monitoring of logs helped us in identifying new trends/methodologies adopted by hackers.

9. Scientific and technological methodologies used in work function.

System administration:-
- Locality-based cluster in Active-Passive mode has configured on Solaris10 OS.
- Mail server configured in cluster environment, IP based switching was used in this cluster configuration
- Multiple Resource Group created for automated switching of services between servers.
• Security for mail server enhanced by putting policies in Gateway server.
• Internet connectivity from multiple vendors ensured high availability.
• Logs stored in a separate directory for the analysis purpose.

Domain controller Administration:-
• Creating user, locking and unlocking user accounts, resetting passwords, privilege management, revoking system privileges, granting and revoking roles.

Intrusion Detection and prevention System
• Snort

Network management/Analysis
• Security Information and Event Management (SIEM) Tool (RSA envision Appliance)
• HP Webinspect, IBM Rational Appscan, Saint, Nessus, GFI Languard

Incident Handling
• NIST Incident handling guideline
• CERT/CC Incident handling SOPs
• Whois service and Tools (Smart whois, dnsstuff etc)
• Encryption and Digital Signature (PGP)

10. Suggestions (if any) for work functions based on new or emerging scientific principles.
• A reliable and secured DR system should be implemented.
• Network traffic traverses through CERT-In router may be stored for analysis purpose.
• Malicious data may be stored for research activities.

11. New technologies if any introduced by the officer in work plan/functions
• Intrusion prevention mechanism was introduced on different layers for preventing attacks on CERT-In network.
• Passive packet capturing tools used for analyzing deep packet inspection.
• Signature and Rate based IPS deployed for securing Network.
• New devices & S/W tools incorporated from industry leaders of the respective field.

12. Any other highlight of special S&T content in the work
• Computer Security Incident Handling.
• Software/hardware Mirroring was created between hard disks.
• All critical servers are configured in cluster mode for redundancy and high availability.

13. One page summary of the scientific and technical elements in the work done during the financial year
b) Computer Security Incident Handling.
c) Implementing the active and proactive measures relevant to the vulnerabilities and cyber attacks comes to my knowledge through various sources.
d) Participation in all the National/International Incident Handling and cyber security Drills conducted and participated by CERT-In/CERTs across the world.
e) Daily log analysis of servers and security devices installed to look for any anomaly and take
action.

f) Troubleshoot networks, servers, and applications to identify and correct malfunctions and other operational difficulties.

g) Investigate user problems, identify their source, determine possible solutions, test and implement solutions.

h) Guidance and technical support to the juniors to achieve their goals assigned.

14. Quantified S&T outputs as per the selected indicators (as annexed)

<table>
<thead>
<tr>
<th>Total Score</th>
</tr>
</thead>
</table>

Signature of the officer reported upon