To,

May 08, 2018

DBT Mission, 4th Floor
Shivaji Stadium Annex Building
Rajiv Chowk,
New Delhi: 110001

Subject: Security Assessment of Direct Benefit Transfer (DBT) App (Scheme Management System)

Dear Sir,

PwC has completed Web Application Security Assessment (WASA) of the Direct Benefit Transfer - Scheme Management System (DBT App).

Details of the audit are as follows:

Website Details:	Link are provided below: http://180.151.3.101/dbtapp-v4/
Activity:	Web Application Security Assessment
Audit Performed by:	PwC
Testing Date:	5th Apr – 5th May 2018

Note:

1. Vulnerabilities that arise due to absence of SSL certificate on web server are still in application which will be mitigated by implementing SSL. SSL certificate will be implemented in production environment wherever this application will go-live.
2. Few of the vulnerabilities are still open such as Improper session timeout, Server banner disclosure, Cookie without http only & secure flag, Referrer header is not validated at server side and HSTS is not implemented. These will be fixed once website are deployed on production server by implementing HTTPS using SSL certificate.

Recommendations:

1. In case of any additions/deletion of modules and changes to the source code, it is highly recommended to perform a complete web application security assessment.
2. It is recommended to implement SSL certificate on web server hosting DBT App web application in production environment.
3. It is recommended that complete security assessment of the application be carried out on regular basis.
4. The directory of upload files is /data and necessary R/W permissions have been given to this directory.

Warm Regards,

Rahul Aggarwal
Partner

PricewaterhouseCoopers Pvt. Ltd. pwc Gurgaon