
The system has been assessed by Spherecom using the assessment methods and procedures required by the system’s assessment process as described in CIO-IT Security-6-30 to determine the level of risk associated with operating the system and the effectiveness of the system’s security controls in satisfying the security requirements of the system. A Plan of Action and Milestones (POA&M) has been developed describing the corrective measures implemented or planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.
Authorization to Operate Letter

Based on the level of risk described in the results of Verizon/Cybertrust Shared Service Provider (CYBSSPS)’s security assessment and the planned actions in its POA&M, I recommend authorization of the Verizon/Cybertrust Shared Service Provider (CYBSSPS) information system.

RECOMMEND AUTHORIZATION:

X e-Signed by Joseph Hoyt on 2018-10-15

Joseph Hoyt
Information System Security Manager

After reviewing the results of the security assessment, and the supporting evidence provided in the security authorization package, I have determined the risk to GSA’s Federal systems, data, and/or assets resulting from the operation of the information system is acceptable.

Accordingly, I am issuing an Authorization to Operate (ATO) for the Office of Government-wide Policy Verizon/Cybertrust Shared Service Provider (CYBSSPS) information system in its current environment and configuration. This authorization is valid for Three (3) years from the Authorizing Official’s signature on this letter or until a significant change in the system or threat/risk environment, as described in CIO-IT Security 06-30, necessitates re-assessment and re-authorization. This security authorization has the following conditions:

1. Verizon/Cybertrust Shared Service Provider (CYBSSPS) will decommission RHEL 5 server in use by March 31st, 2019.
2. Verizon/Cybertrust Shared Service Provider (CYBSSPS) shall mitigate residual POA&M action items as identified in the Security Assessment Report and from ongoing continuous monitoring activities.
3. Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guideline, and policy.

APPROVED:

X e-Signed by Dan Pomeroy on 2018-10-15

Dan Pomeroy
Authorizing Official

CONCURRENCE:

X e-Signed by Pranjali Desai on 2018-10-16

Pranjali Desai
Acting Chief Information Security Officer

Copies of the authorization package are available for review at the GSA facilities in the Washington, D.C. metropolitan area. If you have any questions or comments regarding this authorization to operate, please contact Man Lau, Director ISSO Support Division (IST) by email at man.lau@gsa.gov or phone (202) 219-7982.