Office of the Chief Information Officer

June 3, 2013

MEMORANDUM FOR: ELIZABETH F. DELNEGRO
AUTHORIZING OFFICIAL
ACQUISITION IT SERVICES

FROM: ANTHONY C. KONKWO
INFORMATION SYSTEMS SECURITY MANAGER
ACQUISITION IT SERVICES

THRU: KURT D. GARBARS
SENIOR AGENCY INFORMATION SECURITY OFFICER

Subject: Security Authorization Package:
AT&T Managed Trusted Internet Protocol Service

A security controls assessment of the AT&T Managed Trusted Internet Protocol Service (MTIPS) information system was conducted at the FIPS 199 High Impact level in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37 R1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; and the General Services Administration (GSA) Security Authorization Process.

The enclosed security authorization package transmits the AT&T MTIPS Security Assessment Report, System Security Plan, and Plan of Action and Milestones (POA&M), together with the Penetration Testing Report, Contingency Plan, and Contingency Plan Test Report. The security controls listed in the System Security Plan have been independently assessed by Knowledge Consulting Group (KCG), using the assessment methods and procedures described in the Security Assessment Report to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The POA&M describes the corrective measures that have been implemented or are planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

Based on the existing security configuration defined in the System Security Plan, the planned actions in the POA&M, and the stipulations below, I certify that the AT&T MTIPS information system is currently operating at an acceptable level of risk, and recommend authorization through June 3, 2016 conditioned on the following items:

U.S. General Services Administration
2200 Crystal Drive
Arlington, VA 20406-0003
www.gsa.gov

1. AT&T shall resolve all open POA&M items identified during the security assessment process, per the schedule defined in the POA&M and in accordance with GSA IT Security Policy (GSA Order P. 2100.1H).
2. AT&T shall implement a process for conducting privileged authenticated vulnerability scanning no later than September 4, 2013.
3. AT&T shall provide GSA the unedited results of the vulnerability scans on a quarterly basis, in conjunction with the published GSA POA&M schedule.
4. AT&T shall resolve all items identified during the quarterly operating system, database, and web application vulnerability scans in accordance with GSA IT Security Policy (GSA Order P. 2100.1H).
5. The technical recertification activities for the next ATO shall commence no later than six months before the expiration of this ATO.

RECOMMEND APPROVAL:

6/4/2013

X Anthony C. Konkwo

Anthony C. Konkwo
Information System Security Manager

CONCURRENCE:

X Kurt Garbars

Kurt D. Garbars
Senior Agency Information Security Officer

ATTACHMENTS:
Security Assessment Report
System Security Plan
Penetration Test Report
Plan of Action and Milestones
Contingency Plan
Contingency Plan Test Report