Federal Communications Commission
Washington, D.C. 20554

February 16, 2011

DA 11-296

Mr. Scott Barash
Acting CEO
Universal Service Administrative Company
2000 L Street, NW
Washington, DC 20036

Dear Mr. Barash,

With this letter, the Commission provides additional instruction to the Universal Service Administrative Company (USAC) concerning compliance with the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347).[1]

On November 8, 2010, KPMG LLP released the report entitled "FCC Security Program IT General and Application Control Testing Findings and Recommendations" (FISMA Report).[2] As the FISMA Report notes, section 3544(a) of FISMA states that agencies are responsible for providing information security protections for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[3] Section 3544(b) further states that each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[4] The FISMA Report identified a number of instances in which USAC's security program was not being operated consistent with FISMA requirements.[5] In response to these findings, the FISMA Report recommended that USAC:

- perform, at least annually, disaster recovery tests of all its major applications and general support systems used in support of the Commission;
- ensure that all systems under USAC control are re-authorized every three years or when a significant change to the information system occurs;
- document a security authorization letter for the USAC General Support System (GSS) that includes the authorization decision, terms and conditions for the authorization and the authorization termination date;

[1] *See* 44 U.S.C. § 3541, *et seq.*; Letter from Steven VanRoekel, FCC, to Scott Barash, USAC (Apr. 9, 2010) (available at http://www.fcc.gov/omd/usac-letters/2010/040910-FISMA.pdf); Letter from Steven VanRoekel, FCC to Scott Barash, USAC (Oct. 6, 2010) (available at http://www.fcc.gov/omd/usac-letters/2010/100610-FISMA.pdf ).

[2] *See* Federal Communications Commission, *FCC Security Program IT General and Application Control Testing Findings and Recommendations* (Nov. 8, 2010) (FISMA Report).

[3] *See* 44 U.S.C. § 3544(a).

[4] *See id.* § 3544(b).

[5] *See* FISMA Report at 35-37; FISMA Compliance – Oversight of Contractor Systems, *Notice of Findings and Recommendations*, Year Ended September 30, 2010, NFR Number IT-10-11 (detailing the findings cited in the FISMA Report).

- document system security plans in detail sufficient to plan system security controls for general support systems and major applications that are identical or equivalent to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 3 minimum baseline controls;

- consider within its risk assessments a full range of significant risks and include system characteristics, the likelihood rating assigned to each vulnerability, the residual risk to agency operations or agency assets, and the calculation of risk levels. Control recommendations from risk assessments should be used to create or update system security plans;

- test a representative subset of IT security controls (including management, operational, and technical controls) annually for the USAC GSS and major applications so that all controls are assessed at least once during an information system's three-year authorization cycle. For future security assessments in support of initial security authorizations USAC should also ensure that all IT security controls are tested; and

- revise, finalize and implement procedures for completing a security authorization package, including planning and scoping guidance and procedures for creating a security authorization package in accordance with NIST guidance and for administering USAC's security authorization program. USAC's policies and procedures should require that security assessment testing cover a representative subset of management, operational and technical controls in accordance with evaluation criteria from NIST SP 800-53a.[6]

The Commission directs USAC to incorporate the above recommendations into its FISMA compliance procedures and to take the necessary steps to implement these recommendations immediately, including providing the Commission with a corrective action plan in accordance with previous Commission guidance. My staff will be contacting you following the date of this letter to discuss any questions you may have. In addition, please immediately provide us with copies of the complete certification and accreditation packages, including system security plans, Federal Information Processing Standards 199s, and all other artifacts for the USAC GSS and all major applications. Finally, please provide us with a copy of the current USAC Information Systems Security Policy. This information will be forwarded to the FCC ITC Chief Information Security Officer (CISO), Mr. Phillip Ferraro. Should you have any questions on the above, please contact the FCC CISO

Thank you for your efforts to date in response to past Commission directives to comply with FISMA. I look forward to implementation of the above recommendations to further improve USAC's FISMA compliance.

Sincerely,

Steven VanRoekel
Managing Director

Cc: Dana Shaffer
Phillip Ferraro

[6] *See* FISMA Report at 37-38.