Federal Communications Commission
Washington, D.C. 20554

October 6, 2010

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

RE: Application of Federal Information Security Management Act (FISMA)

Dear Mr. Barash,

As follow-up to the Commission's April 9, 2010, directive to USAC to take steps to ensure its compliance with FISMA and notification of the inclusion of systems operated by USAC on the Commission's annual FISMA submission to the Office of Management and Budget, please find the enclosed guidance entitled, "Federal Communications Commission (FCC) Information Technology (IT) Governance Framework and Universal Service Administrative Company (USAC) IT Governance Roadmap."

This information is being provided as part of the collaborative process to assist USAC in meeting FISMA requirements. It also will provide USAC with information to develop a plan to meet compliance with applicable Federal statutes, regulations, and then implement guidance concerning the acquisition, use and monitoring of IT investments, specifically focusing in the areas of Capital Planning Investment and Control (CPIC), System Development Life Cycle (SDLC) documentation, IT Security, and Privacy Management.

Please contact Deputy Managing Director Dana Shaffer if you have questions regarding this information or the April 9th directive.

Sincerely,

Steven VanRoekel
Managing Director

Cc: Sharon Gillett
Mark Stephens
Dana Shaffer
James Greening

Federal Communications Commission (FCC) Information Technology (IT) Governance Framework And Universal Service Administrative Company (USAC) IT Governance Roadmap

Purpose:

The purpose of the Federal Communications Commission (FCC) IT Governance Framework and Universal Service Administrative Company (USAC) IT Governance Roadmap is to communicate established FCC IT governance practices to USAC and provide the USAC with a plan to achieve compliance with applicable statutes, regulations, and implementing guidance concerning the acquisition, use and monitoring of IT investments, specifically focusing in the areas of Capital Planning Investment and Control (CPIC), System Development Life Cycle (SDLC) documentation, IT security, and Privacy Management. The goal is USAC's establishment of an IT Governance structure consistent with the FCC's IT governance activities. The FCC is committed to providing instruction, assisting USAC in updating its IT governance practices, and working with USAC to meet any deadlines associated with reporting for information systems.

Background:

The Federal Information Security Management Act (FISMA) requires the Commission to actively oversee USAC's IT Security Program and to include USAC's IT systems and those of its contractors (including but not limited to Solix and any banking institutions) in the Commission's annual FISMA submission to the Office of Management and Budget (OMB). The applicability of FISMA to USAC and its contractors was communicated to USAC by the FCC's Managing Director on April 9, 2010.

The FCC is expanding its oversight of USAC's and its contractors' IT practices to ensure that the USAC's IT program is consistent with Federal requirements and FCC IT governance practices. Over the coming months the FCC's CIO anticipates meeting with USAC's IT staff on a regular basis to discuss USAC IT governance and to assist USAC by providing guidance and review of its IT policies and practices.

Federal IT Governance Framework:

The following laws, policy and guidance govern the FCC's IT resources. These laws, policies and guidance, in addition to any amendments and updates that may be adopted, also govern USAC's IT resources and investments.

1) **Clinger Cohen Act of 1996, 40 U.S.C. Subtitle III, Chapters 111, 113, 115, and 117,** available at

http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html

The Clinger-Cohen Act requires agencies to establish goals for improving efficiency through the effective use of IT. Agencies must establish performance measurements to assess how well IT supports agency programs. In addition, agency heads must benchmark agency process performance against comparable processes in terms of cost, speed, productivity, and quality of outputs and outcomes. Agency heads must clearly define agency missions and consider appropriate process changes before making significant investments in IT. Agencies must also report annually on operational improvements achieved through the effective use of IT.

2) **The Federal Information Security Management Act of 2002**, 44 U.S.C. § 3541, *et seq.*, available at http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Federal Information Security Management Act of 2002 (FISMA) sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. In addition, FISMA provides a mechanism for improved oversight of federal agency information security programs. This mechanism includes mandated annual reporting by the agencies, the OMB, and the National Institute of Standards and Technology (NIST). FISMA also includes a requirement for independent annual evaluations by the inspectors general (IG) or independent external auditors.

3) **OMB Circular A-11, part 7**, available at http://www.whitehouse.gov/omb/assets/a11_current_year/part7.pdf.

The OMB Circular A-11 establishes policy for planning, budgeting, acquisition and management of Federal capital assets, and provides instruction on budget justification and reporting requirements for major IT investments and major non-IT capital assets.

4) **OMB Circular No. A-130 and revisions including Transmittal No. 4**, available at http://www.ogc.doc.gov/ogc/contracts/cld/ecomm/65fr77677.html

This OMB Circular establishes policy for the management of Federal information resources, including procedural and analytic guidelines for implementing specific aspects of these policies. It covers the acquisition, use, and disposal of information technology as a capital asset by the Federal government to improve the productivity, efficiency, and effectiveness of Federal programs.

5) **NIST Special Publication 800-37, Revision 1. Guide for Applying the Risk Management Framework to Federal Information Systems**, available at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

This document is a guide for applying the Risk Management Framework to Federal IT Systems and it follows a security life cycle approach to managing those assets. The

National Institute of Standards and Technology (NIST) has developed a common information security framework for the federal government and its contractors to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies. This publication emphasizes (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

6) **NIST Special publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**, available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

This document provides guidelines for a risk-based approach to protecting the confidentiality of PII, which is defined as any information about an individual maintained by an agency including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Each agency is subject to Federal statutes, laws and regulations governing privacy, including; OMB requirements (including OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003) (http://www.whitehouse.gov/omb/memoranda_m03-22/); OMB Memorandum M-07-16, May 22, 2007; Safeguarding Against and Responding to the Breach of Personally Identifiable Information, available at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf; and the Privacy Act (5 U.S.C.552a), for protecting PII. Therefore, an agency's legal counsel and privacy officer should be consulted to identify current obligations for PII protection.

7) **OMB Memorandum M-10-15, April 21, 2010; FY 2010; Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management** available at http://www.cio.gov/documents_details.cfm/uid/255D3B21-BDBE-6B59-F6B975525A6C0532/structure/OMB%20Documents%20and%20Guidance/category/Policy%20Letters%20and%20Memos;

This memorandum provides instructions to agencies for meeting their FY 2010 reporting requirements under the FISMA. Each agency is to include all of its information systems in its FISMA report. The memorandum also includes reporting instructions on an agency's privacy management program. In addition, the Department of Homeland Security (DHS) will provide additional operational support to Federal agencies in securing Federal systems which the Commission will

communicate, as appropriate, to USAC. DHS will monitor and report agency progress to ensure the effective implementation of this guidance.

For FY 2010, FISMA reporting for agencies will be accomplished through CyberScope, the platform for the FY 2010 FISMA submission process. The Commission will coordinate with USAC concerning the use of CyberScope to report USAC's IT systems.

FCC IT Governance Framework:

The FCC's current IT Governance Framework as of October, 2009, meets the requirements of applicable Federal statutes and guidance set forth by OMB. The FCC Information Technology Center (ITC) governance practices include an IT Strategic Plan, an established CPIC process, SDLC Process, IT Security considerations, and portfolio management and reviews. These processes and practices are continuously modified to adjust to changing federal requirements and mature ITC's governance capabilities.

The FCC established the ITC to manage and direct all IT activities of the FCC. The ITC coordinates various policies and guidelines which are established by the Chairman and the Managing Director and ensures that they are followed. It is responsible for the overall direction of Commission programs involving the use of computer and telecommunications systems. The FCC's, Chief Information Officer (CIO) is the senior manager of the ITC.

The FCC also has an Executive Review Committee (ERC) and an Information Technology Steering Committee (ITSC). The ERC reviews recommendations on IT investments and makes key investment decisions on the Agencies' investment portfolio. The ITSC is a cross-functional executive review committee responsible for the FCC's IT Investment Portfolio.

IT Governance Documentation

Documented IT governance practices are fundamental in communicating expectations to all parties involved in the various processes and establishing repeatable standards. The following items identify FCC documents that support its governance practices. These documents will be made available to the USAC (and kept confidential as appropriate under the confidentiality provisions of the Memorandum of Understanding between USAC and the Commission) and may be utilized and modified by the USAC as needed.

1) *Federal Communications Commission IT Strategic Plan, FY 2008-2012;* October 2007, available at http://www.fcc.gov/omd/strategicplan/InfoTechnologyPlansandReports/itsp2008-2012.pdf. The IT Strategic Plan (ITSP) sets forth the current and future foundation and guidelines that direct Commission-wide IT activities for building an information

systems architecture that is increasingly interoperable and migrates toward a single vision of IT at the FCC.

2) *FCC Information Security Program – FCC Directive, FCCINST 1479.3*, July 2008.
The FCC Information Security Directive discusses policy and assigns responsibilities for assuring that there are adequate levels of protection for all FCC information systems, the FCC Network, applications and databases, and information created, stored, or processed.

3) *Federal Communications Commission (FCC) Information Technology Capital Planning and Investment Control (CPIC) Guide*; Ver. 2.0.0, October, 2009.
This guide documents the FCC's Capital Planning and Investment Control (CPIC) process for IT and provides decision-making guidance. The CPIC guide provides the process to align the IT Investment Portfolio with the FCC strategic plan, and ensures a consistent, effective, and efficient process is applied through the selection, evaluation, and control phases of FCC IT Investments.

4) *Federal Communications Commission (FCC) Information Technology Center (ITC) Enterprise Life Cycle (ELC);* October, 2009.
This is a diagram of the entire ELC workflow, including the CPIC process, the IT Request Process, and the SDLC.

5) *Roles and Responsibilities for the System Development Life Cycle (SDLC);* Ver. 1.2, October, 2009.
The purpose of this document is to distinguish the various responsibilities of Information System Owners (ISOs), Information Owner/Steward (IO/Ss), Contracting Officer's Technical Representatives (COTRs) and Chief Information Security Officer (CISO), and to enable them to work cooperatively as they develop, administer and manage the FCC information systems. This document provides guidance and establishes procedures for ISOs, IO/Ss, COTRs and CISO to help implement proper planning, control, development, testing, security and operations of their assigned systems over the systems' life cycle. Specifically, this guide:

- promotes the overall awareness of the responsibilities of FCC ISOs, IO/Ss, COTRs and CISO;
- provides further guidance on the responsibilities for the various roles associated with information system ownership;
- provides more specific information regarding ISO, IO/S, COTR, and CISO roles and responsibilities as defined in the FCC Security Directive 1479.3;
- provides guidance on technical updates to systems;
- provides guidance on security configuration and account management; and
- answers general questions about FCC's directives, policies, and processes pertaining to systems development and operations; and identifies Federal

regulations that set standards and guidance for the security of FCC's information systems.

6) *Standard Operating Procedures (SOP) for Information Technology (IT) Project Requests, Version 1.0.1, Effective date April, 2010.*
This document provides the work flow and SOP for requesting IT goods and services within the FCC. There are two types of requests:

- IT Requests for projects with allocated funding for the current fiscal year's budget.
- IT Requests for current or future budgets where funding has not yet been requested or allocated.

This document assists FCC staff in completing the necessary documentation and performing planning functions in order to receive IT goods and services.

7) IT Request Form (FCC Form A-109)
The IT Request Form is used by FCC Bureaus and Offices (B/O) to request approval for IT projects or requests (goods and services) that have been identified as potential needs. See #6, *Standard Operating Procedures (SOP) for Information Technology (IT) Project Requests, Version 1.0.1, April, 2010.* The form provides a standard way for management to evaluate IT requests and can be used for evaluation and approval by an identified person or group such as an IT Program Manager/Office.

USAC IT Governance Roadmap:

The purpose of this portion of the document is to advise USAC regarding IT Governance and how it can comply with that guidance. USAC must establish an IT Governance structure consistent with the FCC ITC's governance activities, although it need not be identical. The FCC is committed to providing instruction and assisting the USAC in updating its IT governance practices.

The FCC understands that USAC will need time to evaluate its own IT Governance Policies and Procedures and then some additional time to establish new and updated ones. The FCC will work with USAC to expeditiously update its IT governance practices.

Review of USAC's IT Governance Structure:

The FCC plans to monitor and ensure that the USAC enhances its IT Governance structure. The FCC will meet periodically with USAC IT staff to review various IT topics and provide guidance to help USAC achieve compliance in the acquisition and monitoring of IT investments. During this process, the FCC and USAC will undertake the following:

1. USAC will share with the FCC the current IT practices and supporting documentation;

2. FCC will review documentation and note inconsistencies with Federal guidance or FCC practices;
3. FCC and USAC will work together to identify and develop a strategy for addressing areas that require improvement;
4. FCC and USAC will agree upon plans and timeframes for finalizing USAC IT Governance practices;
5. USAC will implement practices to manage its IT Strategic, CPIC, SDLC, and IT Security activities;
6. FCC will periodically review and assesses USAC IT Governance practices; and
7. FCC and USAC will work together to coordinate policies and practices for Privacy Management, *i.e.*, privacy training, systems of records, privacy impact assessment, and breach notifications.

Review of Specific USAC IT activities:

The FCC has identified current USAC IT activities practices and policies, which the FCC will evaluate to determine whether they are consistent with FISMA and implementing Federal guidelines. The FCC has selected the activities, practices and policies in the following list for initial evaluation:

- USAC IT purchases (IT equipment, software, licenses and delivered services).
- USAC IT Contract Procurements (It is FCC's understanding that over 20+ IT Procurements have been awarded, are in process, or are scheduled and identified for award).
- USAC IT Security, FISMA Activities, and Privacy Management.
- USAC's policy and use of Government Furnished Equipment (GFE) and Rules of Behavior.

Contact Between the FCC and the USAC:

The FCC has designated James (Jim) Greening, Associate CIO, as the FCC ITC official point of contact for all IT related USAC communications. USAC may contact Jim Greening, and funnel any inquiries or document transmissions through him, as needed. Other FCC officials involved in the oversight of USAC IT practices include:

- Dana Schaffer, Deputy Managing Director
- Phillip Ferraro, FCC ITC Chief Information Security Officer (CISO)
- Jill Goldberger, FCC ITC Deputy CIO for IT Governance
- Rita Cookmeyer, FCC ITC Program Manager responsible for the Program Management Office
- Leslie (Les) Smith, FCC Privacy Analyst responsible for Privacy Issues
- Larry Schecker, Legal Advisor for Privacy