FEDERAL COMMUNICATIONS COMMISSION
Washington, D. C. 20554
APR 9 2010

OFFICE OF
MANAGING DIRECTOR

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 you may know, the Federal Information Security Management Act of 2002 (FISMA) "provide[s] a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."[1] In guidance to agencies implementing the FISMA, OMB has explained that it covers "entities … which operate on behalf of Federal agencies, to collect, create, process, or maintain Federal government information."[2] Accordingly, "[a]gency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) -- on behalf of a Federal agency."[3]

The Commission's annual financial statement for fiscal year (FY) 2009 was recently audited by KPMG, LLP. As part of the audit, KPMG examined the FCC's FISMA compliance, and the applicability of FISMA to FCC components was brought to our attention. Specifically, KPMG found that the FCC had "not formally determined and documented its responsibilities for directing and overseeing the information security programs for information systems that collect and maintain FCC data but are not operated by the FCC" including those operated by the Universal Service Administrative Company (USAC).[4] Accordingly, we undertook our own analysis and determined that the FISMA does indeed require the Commission to actively oversee USAC's IT Security Program and to include systems operated by or on behalf of the FCC on the Commission's annual FISMA submission to the Office of Management and Budget. This determination applies to USAC and any of its contractors or other service providers, including but not limited to Solix and any banking institutions, that have access to FCC data.

---

[1] 44 U.S.C. §§ 3541, *et seq*.
[2] Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-09-29 (Aug. 20, 2009) (OMB FISMA Memo) at 9-10.
[3] OMB FISMA Memo at 16.
[4] Notice of Findings and Recommendations (NFR) number IT-09-11, KPMG, attached.

Therefore, the Commission directs USAC to take steps to ensure that it complies with FISMA, to work with the FCC in completing the annual FISMA audit beginning with this fiscal year, and to implement recommendations 2 through 6 in the attached NFR. These actions will build upon and bring into full compliance with FISMA the steps that the Commission's CIO and CFO have taken in past years to review the operation of USAC's information systems. This directive is also consistent with Section IV.G.1 of the Memorandum of Understanding between the FCC and USAC (MOU), which provides that USAC "will comply to the fullest extent possible . . . with federal and Commission information technology requirements . . . including computer and information security . . . . This may include IT related legislative requirements . . . , Presidential/OMB directives . . . and other federal mandates."

Additional guidance and information about meeting the FISMA requirements can be found in Office of Management and Budget (OMB) Circular No. A-130, Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, M-09-29 (Aug. 20, 2009) issued by OMB and in the attached document. My staff will be contacting you soon to set up a meeting to begin the collaborative process needed to determine all the steps necessary to accomplish this task. In the meantime, please contact Andrew Martin, Chief Information Officer, (202) 418-2020, if you have any questions about this directive.

Sincerely,

Steven Van Roekel
Managing Director

Cc: Andrew Martin
Sharon Gillett
Mark Stephens

Notice of Findings and Recommendations

Federal Communications Commission (FCC)
Notice of Finding and Recommendation (NFR)
Year Ended September 30, 2009

Background:

KPMG Auditor:	Bill Swiscoski
NFR number:	**IT-09-11**
Program:	IT General Controls
Audit Area:	FISMA Compliance – Oversight of Contractor Systems
PY Audit Finding:	**Yes**
PY NFR number:	NFR # 1, 5, 16
Current Status:	Open
Subject:	Oversight of Contractors
W/P Reference:	U.I.1, U.I.5, S.A.2

Timeline:

Date Finding Provided to OIG:	*August 13, 2009*
Date Finding Provided to Management:	*September 3, 2009*
Date Response Due from Management:	*September 11, 2009*
Date Response Received from Management:	*October 2, 2009*

Condition:

1. The FCC has not formally determined and documented its responsibilities for directing and overseeing the information security programs for information systems that collect and maintain FCC data but are not operated by the FCC to ensure they are administered consistent with all relevant FCC, NIST and OMB requirements and instructions. The systems include those operated by the Universal Service Administrative Company (USAC), National Exchange Carrier Association (NECA) and Welch LLP.

2. USAC maintains an inventory of contractor information systems, however, the inventory does not include an identification of the interfaces between each system and all other systems or networks.

3. USAC's four major applications and one general support system which are used to process FCC data do not have a current certification and accreditation. These five systems, all of which were last certified and accredited on October 2005, are:

    - The Accounting, Billing, Collection and Disbursement (ABCD) application
    - The Disbursement Aggregation System (DAS)
    - The Red-Light (RL) Application

- Microsoft Great Plains
- The USAC general support system

4. Four other major applications used by USAC's service providers (Solix and Telcordia) to process FCC data have not been certified and accredited. These systems are:

    - The Schools and Libraries Division application (SLD) – used by Solix
    - The Rural Health Care application (RHC) – used by Solix
    - The High Cost Program application (HCP) – used by Telcordia
    - The Low Income Program application (LCP) – used by Telcoridia

5. USAC did not perform disaster recovery tests of its major applications and computer information systems.

6. USAC's service provider, Solix, does not have documented Security Awareness Program and Training procedures and has not implemented security awareness training.

Criteria:

Section 3544 of FISMA states that "... *The head of each agency shall – "(1) be responsible for – "(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of – "(i)* ***information collected or maintained by or on behalf of the agency; and "(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;*** *"... Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), 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*** *..." (emphasis added)* [Condition 1]

Section 3543 of FISMA states that the Director of the Office of Management and Budget "... *shall oversee agency information security policies and practices, including – ... (2) requiring agencies, ... to identify and provide information security protections commensurate with the risk and magnitude harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of – "(A)* ***information collected or maintained by or on behalf of an agency; or "(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency*** *..." (emphasis added).* [Condition 1]

OMB Memorandum 08-21 *"FY 2008 FISMA Reporting Instructions"*, in its Frequently Asked Question (FAQ) section further clarifies the applicability of FISMA requirements in its response to question 35: "...Because ***FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources***, it has somewhat broader applicability than prior security law. That is, ***agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency***. Such other organizations may include contractors, grantees, State and local Governments, industry partners, providers of software subscription services, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing Government information and interconnecting systems. *(emphasis added)* [Condition 1]

The MOU between the FCC and USAC states in Section IV.G.1 that: *"The USF Administrator will comply to the fullest extent possible as a non-federal entity with federal and Commission information technology*

*requirements on an ongoing basis including, but not limited to, those pertaining to capital planning, **computer and information security**, communications, and privacy. This may include IT related **legislative requirements**, policies, Presidential/OMB directives, Government Accountability Office ("GAO") recommendations, and other federal mandates." (emphasis added)*
[Condition 1]

The Federal Information Security Management Act of 2002, Section 3505 states that:

> INVENTORY OF MAJOR INFORMATION SYSTEMS – (1) The head of each agency shall develop and maintain an inventory of major information systems ... operated by or under the control of such agency. (2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. (3) Such inventory shall be— (A) updated at least annually; (B) made available to the Comptroller General; and (C) used to support information resources management, including ... (ii) information technology planning, budgeting, acquisition, and management ... (iii) monitoring, testing, and evaluation of information security controls ...
> [Condition 2]

Appendix III to OMB Circular No. A-130, *Security of Federal Automated Information Resources*, states:

> Authorize Processing. A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk and magnitude of harm is high. [Conditions 3 and 4]

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* states that:

> Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; ... (iii) authorize the operation of organizational information systems and any associated information system connections; ... [Conditions 3 and 4]

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* states that:

> Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations. [Condition 5]

NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems*, states:

> CP-4 CONTINGENCY PLAN TESTING AND EXERCISES ... The organization:
> Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and Reviews the contingency plan test/exercise results and initiates corrective actions. [Condition 5]

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* states that:

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. [Condition 6]

Cause:

FCC management has informally taken the position that FISMA does not require it to oversee the information security program for systems operated on behalf of the FCC by USAC, NECA and Welch LLP. Before deciding whether to modify that position, the FCC is seeking guidance from its Office of General Counsel on whether FISMA requires the FCC to actively oversee USAC's IT Security Program and to include USAC systems operated on behalf of the FCC as contractor systems on the Commission's annual FISMA submission to OMB. Based on that decision, the FCC plans to document its responsibilities for information systems operated by any third-party on behalf of the FCC.

FCC does not have policies and procedures in place regarding the oversight and evaluation of information systems used or operated by a contractor of the agency or other organization (e.g., USAC) on behalf of the agency.

Neither FCC nor USAC have established policies and procedures for maintaining an inventory of contractor information systems operated on behalf of the FCC.

Effect:

By not including systems operated on behalf of the FCC by third parties, the FCC's system inventory may be incomplete. Not including USAC and other contractor systems on the Commission's annual submission to OMB may place the Commission out of compliance with FISMA reporting requirements.

As a result of the FCC not exercising active oversight of USAC's IT security program, USAC information systems that process FCC data may be operated without the information security controls required by FCC policy or FISMA. As a result, FCC data processed on behalf of the Commission by USAC may be subject to unauthorized use, loss, or disclosure.

As a result of the FCC not exercising active oversight of the IT security programs of other contractors that operate systems that collect or maintain FCC data, contractor systems that process FCC data may be operated without the information security controls required by FCC policy or FISMA. As a result, FCC data processed on behalf of the Commission may be subject to unauthorized use, loss, or disclosure.

Federal Communications Commission
Notice of Finding and Recommendation (NFR)
Year Ended September 30, 2009

Recommendation:

We recommend that the FCC Chairman and the FCC Chief Information Officer (CIO) ensure that:

1. The FCC formally documents its responsibilities for directing and overseeing the information security programs for information systems that collect and maintain FCC data, but are not operated by the FCC, to ensure they are administered consistent with all relevant FCC, NIST and OMB requirements and instructions.

2. The FCC and USAC should establish procedures for maintaining an inventory of contractor information systems operated on behalf of the FCC, including the documentation of interfaces between major applications and all other systems or networks.

3. USAC certifies and accredits all systems under USAC control (either directly or through other service organizations) that process or hold FCC data.

4. USAC performs at least annually, disaster recovery tests of its all major applications and general support systems used in support of FCC.

5. USAC requires the USAC service provider Solix to document and implement security awareness program and training procedures.

Auditee's Response:

_____ Management concurs with the factual accuracy of finding.

_____ Management does not concur with the factual accuracy of finding.

This NFR presents both a significant departure from historical treatment of third-party entities and a material change to the relationship between those entities and the Commission. Prior to determining concurrence or non-concurrence with this item, management is consulting with Counsel to ensure that we do not unintentionally create obligations or regulations that should be reserved for Commission-level determinations.

Please indicate your response in the space provided above or as an attachment within one week from the date of this notification. Your written response will be considered when preparing the draft audit report.

Federal Communications Commission
Notice of Finding and Recommendation (NFR)
Year Ended September 30, 2009

Signature of Senior	Signature of Auditee Official
Signature of Site Manager	Title of Auditee Official

Waiting for OGC Response.

12/4/09

Finding Disposition:

__X__ **Management letter comment**

_____ **Significant Deficiency in internal controls**

_____ **Material weakness in internal controls**

_____ **Non-compliance with laws and regulations**

All EDP findings will be accumulated and a level assessed upon completion of all EDP-related test work. A combination of related management letter comments may result in a significant deficiency, material weakness, or noncompliance with laws and regulations. In addition, a combination of related significant deficiency conditions may result in a material weakness.