

CONFIDENTIAL DATA ACCESS ISSUES FOR AUDITORS AND EVALUATORS

THURSDAY, DECEMBER 15, 2016
3:00 PM ET/ 2:00 PM CT/1:00 PM
MT/ NOON PT



Moderator



Katrin Osterhaus is originally from Germany and came to the United States as a foreign exchange student. After receiving her master's degree in business administration, she was hired as a performance auditor with the Kansas Legislative Division of Post Audit in 1998. During her tenure, Katrin participated in and supervised performance audits on a wide variety of topics. She attained the Certified Internal Auditor (CIA) and Certified Government Auditing Professional (CGAP) designations, and most recently passed the Project Management Professional (PMP) certification. In her current role as IT Audit manager, she's responsible for overseeing her team's work on IT security audits, as well as monitoring ongoing IT projects that state agencies are executing.



Speakers



Dr. Jon Courtney, program evaluation manager, New Mexico Legislative Finance Committee



Justin Stowe, deputy post auditor, Kansas Legislative Division of Post Audit



Ted Booth, general counsel, Mississippi Joint Legislative Performance Evaluation and Expenditure Review Committee



Speaker



Dr. Jon Courtney holds a PhD in experimental psychology from Texas Christian University, and currently serves as the Program Evaluation Manager for the New Mexico Legislative Finance Committee. Jon has 10 years of experience in program evaluation having served the state of New Mexico for 8 years and having previously served as a Principal Scientist for General Dynamics. Under Jon's leadership, the Legislative Finance Committee staff have been recipients of the Excellence in Research Methods and Excellence in Evaluation Awards from the National Legislative Program Evaluation Society.





NEW MEXICO
LEGISLATIVE
FINANCE
COMMITTEE

Data Access in NM

Jon Courtney
Program Evaluation Manager
New Mexico Legislative Finance Committee

Overview



Data Access in NM

- ▶ Statutory authority
- ▶ Educating staff and agencies
- ▶ Overcoming delays and denials
- ▶ What works and what doesn't

What we are striving for...

- ▶ To obtain data and perform analyses that informs Legislators and other stakeholders of the public policy issue at hand
- ▶ The agency should be well informed of our data protections
- ▶ The agency should feel comfortable sharing data
- ▶ The agency should get something from the project when possible
- ▶ LFC staff should be minimally intrusive and provide adequate protections for data

Statutory Authority



- ▶ LFC has broad statutory authority to examine and evaluate the finances and operation of all departments, agencies, and institutions of New Mexico and all of its political subdivisions.

- ▶ Statute provides LFC authority:
 - to receive any information not made confidential by law upon request
 - for all governmental units to cooperate with LFC functions, providing subpoena power in instances of non-cooperation

Educating our staff and agencies

- ▶ LFC staff are trained on educating agencies on access to information:
 - Evaluators share a pamphlet at the beginning of a project
 - “What to expect during your program evaluation”
 - LFC staff discuss the following with agencies:
 - LFC’s statutory authority
 - Agency resources
 - LFC’s use of and protections for confidential data
 - Upfront concerns from agency staff around data sharing



Educating our staff and agencies

- ▶ LFC staff set up a structured process for data requests making expectations clear:
 - Use of a tracking form for requests with dates, POCs, and notes
 - Establishment of a timeline for data requests (5 working days)
 - Establishment of one POC at agency and one POC at LFC for requests
 - Establishment of the escalation process for delays or denials



When data is confidential by law

- ▶ LFC asks for confidential information only when necessary
- ▶ Most common types of confidential information:
 - FERPA related
 - Cases “sealed” by law (juvenile justice, adoption)
 - Other grey areas...
- ▶ Most often an agency will agree to provide data by either de-identifying data or signing a memorandum of understanding (MOU)
- ▶ Sometimes de-identification will not suffice



MOUs and Confidential Data

- ▶ Memorandum of Understanding: formal written agreement laying out expectations of LFC and the state agency
- ▶ LFC uses MOUs on a regular basis
 - Advantages:
 - Sets expectations for agencies and LFC
 - Ensures agencies understand all LFC procedures and protections for confidential data
 - Helps set precedent for future data requests
 - Disadvantages:
 - Can be time consuming (legal review)
 - Sets precedent for data being “confidential”

Delays in response



- ▶ Sometimes agencies will agree to provide info but will delay or claim miscommunication
 - Formal **data tracking sheet** with dates and notes
 - Documentation
 - LFC evaluators are encouraged to establish a presence at the agency and ask for info in person
 - Evaluators can use budget analysts to find out reasons for delay and reiterate requests

Denials



- ▶ Denials of data requests come in three forms:
 - 1. Resource related denials
 - The story: Agency cannot provide data as requested due to lack of resources
 - How we address: Offer to receive larger data dump, do work of merging, cleaning, etc on our end
 - 2. Denials based on concerns with confidentiality
 - The story: State or federal law does not allow sharing
 - How we address: Work with agencies to find workaround (de-identification or MOU)
 - 3. Data do not exist
 - The story: Agency does not collect requested data.
 - How we address: Confirm non-existence, work with agency to find an acceptable proxy

Escalation Process

- ▶ If an agency does not respond in the required timeline evaluators notify management.
- ▶ Escalation steps:
 - Management inquiry to agency
 - Formal meeting involving agency secretary and LFC director
 - Potential process related consequences (e.g. budget adjustment requests)
 - Subpoena of information

Strategies for success

▶ What works

- Asking for data in person
- Finding out what data is available before the request is made
 - Looking to other sources (Feds, public reporting, societies)
- Having agency focused on being solutions based

▶ What doesn't

- Relying on email or phone for requests
- Asking for something that is already publically available
- Escalating too quickly or without good cause
- Challenging whether or not something is *confidential*



NEW MEXICO
LEGISLATIVE
FINANCE
COMMITTEE

Thank You

Jon Courtney
Program Evaluation Manager
Legislative Finance Committee
505-986-4550

jon.courtney@nmlegis.gov

Speaker



Justin Stowe currently serves as the Deputy Post Auditor with Legislative Post Audit in Kansas. In that role, he manages several performance audit teams, works with individual legislators and legislative committees to develop audit requests, and assists with the development of the Division's audit policies and procedures. Justin holds certifications as a Certified Government Auditing Professional (CGAP) and a Project Management Professional (PMP), and received his bachelor's degree in political science and a Masters of Public Administration from Kansas State University. When he's not working, Justin enjoys spending time with his family, reading, and learning Tae Kwon Do.



Confidential Data Access

Justin Stowe, Deputy Post Auditor

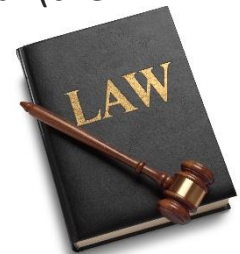
Kansas

Presentation Roadmap

- Statutory Authority for Access
- Making our Access Clear
 - To our staff
 - To our auditees
- Handling Denials of Access
 - Flat-out denials
 - Passive-aggressive denials
- Closing Thoughts & Questions

Statutory Authority for Access

- **Our statutes give us broad access to agency records.** Our statutes give us access to all books, accounts, records, files, documents and correspondence, *confidential or otherwise*. [KSA 46-1106 and 46-1114(d)]
 - Access is restricted to the audit scope
 - Staff have the same duty of confidentiality as auditee staff
- **Our statutes also give us powerful tools of persuasion.** [KSA 46-1115 – 1116]
 - Agencies that fail to furnish records or files to the Division within 30 days of the request can have all agency funds withheld until the records are provided. (the “nuclear” option)
 - Failure to furnish records also is a class A misdemeanor.



Making our Access Clear to Staff | Onboarding

- Our **training module** on laws and data access during the first week on the job (trainer emphasizes that our data access is a great power and a great responsibility). Several other modules deal with confidentiality and security awareness.
- Having new staff **sign confidentiality acknowledgements** and acceptable use agreements help reinforce the importance of keeping confidential information private and safe.
- **Pairing up** new staff with a designated mentor to discuss any questions can help resolve any remaining questions.

Making our Access Clear to Staff | Policies

- **Security clearances** restrict access to the most sensitive datasets [H01.02]
- **Confidentiality** policies define how confidential information is collected, stored, used, and deleted [H02.01]
- **Federal dataset** policies outline some of the specific confidentiality issues related to collecting information made confidential by federal law (HIPAA, FERPA, PHI, etc.) [B04.01.09]
- Our **denials of access** policy lays out our process for staff should handle any denials of access from auditees (we'll discuss this in more detail later). [B04.01.08]

The big one!



Making our Access Clear to Staff | Big Picture

- **Planning**

- Administrative checklist reminds staff to read the policies associated with handling confidential data and developing confidential workpapers
- Entrance conference agendas remind everyone of our access
- Our confidential data planning assessment requires the team to ID any potential confidential data they think they might need for the audit

- **Fieldwork**

- Work with officials to get confidential data sets and identify what state or federal laws make them confidential
- Track all confidential datasets we collect and note any specific rules for data retention or destruction that may be governed by an agency MOU

- **Wrap-up**

- Ensure all confidential material has been appropriately handled (confidential material is to be removed, segregated or obscured as appropriate)
- Segregate all confidential workpapers from our public workpapers once the audit is completed

Making our Access Clear to Auditees

We consistently remind auditees of our access to confidential data throughout the audit to help reduce any confusion or resistance throughout the process.

- Our **audit start-up letter** makes it clear that we have access to confidential information and that we have to protect it.
- Our **entrance conference agenda** includes a specific item regarding confidential data and our access to it.
- Our **auditee brochure** includes a section specific to our access to information.
- Our **data request** letters make it clear that we need to know if any requested information is confidential and

Example: Start-up Letter



LEGISLATURE OF KANSAS
LEGISLATIVE DIVISION OF POST AUDIT

800 SOUTHWEST JACKSON STREET, SUITE 1200
TOPEKA, KANSAS 66612-2212
TELEPHONE (785) 296-3792
FAX (785) 296-4482
WWW.KSLPA.ORG

DATE

AGENCY HEAD, TITLE
AGENCY
STREET ADDRESS
CITY, STATE ZIPCODE

Dear Mr./Ms./Dr. AGENCY HEAD:

At its DATE meeting, the Legislative Post Audit Committee approved an audit examining AUDIT TOPIC. The scope of the work the committee has requested is outlined in the enclosed scope statement.

Also enclosed is a copy of our *Guide for Audited Agencies* document. It provides background information about our agency and summarizes how we conduct our work. There are two specific things about our process that I would like to call to your attention:

- **Access to staff.** Audit standards require that we have full and unmonitored access to staff in agencies we audit. This helps to ensure our audit work is independent and free from any sort of bias. We recognize our responsibility to minimize our intrusion on your staff's time and to work around their schedules. Our goal is to disrupt their work as little as possible, while still meeting our audit goals and deadlines.
- **Access to records.** The Legislative Post Audit Act gives us access to a wide range of information when conducting our audits, including information that is confidential by law. Please let us know if any of the information we request during this audit is confidential by law or has been formally closed by your agency under the Kansas Open Records Act. That way we can take the appropriate steps to keep such information confidential or closed. While the Legislative Post Audit Act gives us access to confidential information, it also makes us subject to the same confidentiality requirements as your agency.

Example: Auditee Brochure

The Legislative Division of Post Audit What We Do and How We Do It: A Guide for Audited Agencies

INTRODUCTION

The information presented here is intended to provide you with a broad understanding of the role of the Legislative Division of Post Audit and its procedures for conducting performance audits.

WHO WE ARE

The Legislative Division of Post Audit is a staff agency of the Kansas Legislature. The Division works under the direction of the Legislative Post Auditor, who is appointed by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a 10-member bipartisan committee of the Kansas Legislature. The Committee considers performance audit topics submitted by Committee members, other legislators, and legislative committees. Performance audits are carried out by the Division only at the direction of the Legislative Post Audit Committee.

WHAT WE DO

The Legislative Division of Post Audit conducts performance audits to determine the efficiency, effectiveness, economy, or results of governmental agencies or programs, or to provide other specific information about those agencies or programs. Performance audits provide the Legislature and agency management with independent analysis, evaluation, and recommendations regarding the performance of the audited activities.

The Legislative Division of Post Audit follows all requirements for conducting performance audits established by the U.S. Government Accountability Office. Statutes governing the Division's authority are set out in K.S.A. 46-1101 *et seq.*

ACCESS TO INFORMATION

Kansas law (K.S.A. 46-1106 and 46-1114(d)) gives the Legislative Division of Post Audit access to agency or program records including all books, accounts, records, files, documents, and correspondence, confidential or otherwise, for the purpose of conducting performance audits. Audit staff are subject to the same penalties as agency staff regarding any unauthorized release of confidential information.

1. Preliminary planning: Once Legislative Post Audit is assigned a topic by the Legislative Post Audit Committee, appropriate agency heads are notified and sent a copy of the approved audit "scope statement," a brief document that describes the questions the audit will seek to answer. Division staff then begin gathering background information and planning the audit. Division staff and management also meet with agency officials. The purpose of the meeting is to allow agency officials to learn about the audit, meet audit staff, discuss any scheduling conflicts, suggest particular areas for audit and investigation, and designate an agency contact person.

2. Field Work: Once the work plan has been approved, the audit team collects information, observes activities, reviews and tests agency data or processes, and evaluates the results of the various analyses. Often the audit team can retrieve data from files and computer records with minimal assistance from the agency staff. In other cases, field work involves observing staff while on the job, interviewing staff and clients, and other techniques that may require agency staff time.

The audit team prepares working papers to document its findings. These working papers are kept confidential in the Division's offices during the audit process. After an audit is completed and has been presented to the Committee, as explained below, the working papers become public documents. However, the public working papers don't contain any information that remains confidential by law.

3. Report: Once the field work is completed, the audit team and the audit manager meet with agency officials to describe the major findings disclosed by the field work, and possible recommendations. At that meeting, the agency officials should inform the auditors of any perceived errors in fact or conclusions. This can help clarify important information.

After the meeting, the draft report is sent to the agency for review. This review period gives the agency an opportunity to point out any errors of fact, call attention to additional information that might have been overlooked, and review conclusions and recommendations. The agency then is asked to prepare a formal, written response to the audit. The written response is an important part of the audit process; agency comments are analyzed carefully and are included as an appendix to the completed audit report. In

Handling Denials of Access | Flat-out Denials

Our denial of access policy details our access to information (and our few limitations) and provides staff with a framework for how to handle denials of access to requested information. That process includes three steps:

1. **Explain** our access to auditee.
2. **Evaluate** how important the records are to our audit objectives.
3. **Respond** by either negotiating with the agency or compelling it to comply.

Step 1 – Explain our Access

- Staff notify the supervisor of any denials of access and the supervisor explains our access to confidential information to the auditee. This *usually* resolves the issue.
- If it doesn't, the supervisor notifies the audit manager and Post Auditor and we move to step 2.



Step 2 – Evaluate the Requested Info

If explaining our access to confidential records doesn't work, the audit team (staff, supervisor, manager) meets to evaluate the importance of the records to answering the audit question. We then categorize that information into one of three buckets:

- Records **are not significant** and can be collected through other means (bucket 1).
- Records are significant to the audit **but not critical**, so we can probably still answer the audit question but maybe not as well (bucket 2).
- Records **are critical** to the audit and without it, the audit question cannot be answered (bucket 3).

Step 3 – Respond to the Agency's Denial

Based on how important we think the information is to answering our audit question (determined in step 2), we have a variety of strategies for how we respond to audited agencies.

- **Negotiate with agency officials to convince them to provide the records (strategy 1).** This path can include:

- having the manager or Post Auditor contacting agency officials to negotiate personally
- requesting an opinion from the AG to clarify our access.

- **Negotiate with the third party (federal agencies, etc.) preventing access to records (strategy 2).**

Often, agencies deny us access to records based on federal restrictions. In these cases we may

- ask the agency for a letter that provides the specific federal citation that limits our access and contact information for the appropriate federal official.
- develop an MOU or sign non-disclosure agreements as necessary to gain access.

- **Compel the agency to provide the records (strategy 3).** Compelling the agency to provide information is our most aggressive option for collecting information and is only used for information deemed critical to answering the audit question. Options include:

- Request that our committee subpoena the record on our behalf.
- Suspend the agency's ability to make payments until the records are provided (used only once in 40 + years)

We don't want to take actions that:
 1) aren't necessary 2)
 we aren't actually willing to take.

We use the following matrix to help guide our thought process on how to proceed with denials of access. Because of its long-term consequences, we have rarely used our authority to compel agencies to comply.

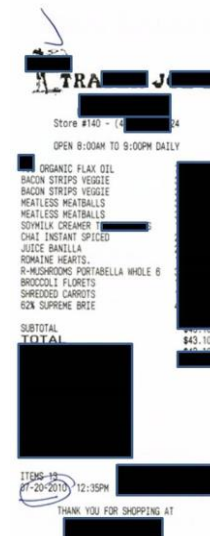
Strategy	IMPORTANCE OF THE INFORMATION		
	Not Significant	Significant	Critical
NEGOTIATE			
The manager contacts the agency to convince officials to provide the records.	X	X	X
The Post Auditor contacts the agency to convince officials to provide the records.	X	X	X
The Post Auditor requests a formal opinion from the Attorney General to convince officials to provide the records.		X	X
COMPEL			
The Post Auditor asks the Legislative Post Audit Committee to issue a subpoena for the records.		X	X
The Post Auditor asks the Legislative Post Audit Committee to formally support suspending the agency's payments until the records are provided.			(a)
(a) The Post Auditor will not consider having the Department of Administration suspend an agency's ability to pay its bills unless three conditions have been met: <ul style="list-style-type: none"> (1) the information must be critical to the audit (i.e., without the information, we cannot conduct a credible audit), (2) all attempts at negotiation and subpoena have failed, and (3) the Legislative Post Audit Committee has formally passed a motion supporting such action. 			

Handling Denials of Access | Passive-Aggressive Responses

In some cases, an agency might agree to provide access to confidential information, but then take a passive-aggressive approach to restricting the information we actually are given. Those actions can include:

- Not providing requested data by the deadline and finding continued reasons to delay
- Not providing the right data despite clear expectations and formal requests
- Providing the data but redacting important information

Regardless of which of these approaches an agency might take, we keep always gauge our response based on the *importance of the information*.



Final Thoughts...

- Do not let your newest employee deal with confidential data requests, but do take them along so they can observe and learn.
- Adjust the level of education regarding access to confidential data to the audited agency.
 - Avoid preaching to agencies that we audit often (because they already understand our access).
 - For smaller agencies or potentially local entities that don't know us as well, we try to overcommunicate our access.
- Set the right tone at the top and be sure to call out your staff if you see confidential information that is not being properly protected. Our reputation depends on taking our rights to confidential access seriously.
- Understand that agencies sometimes simply want to protect themselves by denying access; make it clear that you will take any required and appropriate steps to safeguard what they are giving you.
- Decide whether your office is okay with signing MOUs: once one agency makes you jump through additional hoops, word will spread and it can lead to unforeseen inefficiencies down the road.

Contact information

Justin Stowe, Deputy Post Auditor

Legislative Division of Post Audit

800 SW Jackson, Ste 1200

Topeka, KS 66612

785-296-7977

Justin.stowe@lpa.ks.gov

Speaker



James F. “Ted” Booth is the General Counsel, Mississippi Legislative PEER Committee. He has been an employee of PEER for 32 years. Ted is a member of the Mississippi Bar and American Bar Association. He also served as Staff Co-Chair for the NCSL Redistricting and Elections Committee in 2003-2004, 2006-2008, and 2014-2016.



NATIONAL CONFERENCE *of* STATE LEGISLATURES

Information Access Training and Discussion December 15, 2016

Ted Booth

General Counsel

Mississippi Legislative PEER Committee

Purpose of Presentation

- To provide information on auditor information access issues
- To present and discuss strategies for resolving access issues

Access Rights

- MISS. CODE ANN. Section 5-3-51(b) (1972) provides the following:
- *To conduct, in any manner and at any time deemed appropriate, a review of the budget, files, financial statements, records, documents or other papers, as deemed necessary by the committee, of any agency; to make selected review of any funds expended and programs previously projected by such agency; to investigate any and all salaries, fees, obligations, loans, contracts, or other agreements or other fiscal function or activity of any official or employee thereof (including independent contractors where necessary); and to do any and all things necessary and incidental to the purposes specifically set forth in this section...*

Agency Familiarity With PEER Access Rights

- The larger agencies of state government, and the control agencies, (e. g., the State Auditor, the State Personnel Board) are familiar with our powers, methods, and access rights.
- Smaller agencies of state government provide contractors and local government entities are less familiar.
- Entrance letters set out our statutory rights of access.
- These matters are often discussed in entrance conferences.

Recalcitrance and Escalation

- Some auditees become difficult regarding access.
- Reasons for difficulty include ignorance, possession of information that is not subject to public access, and confidential status of information under state and federal law.

Recalcitrance and Escalation (cont'd.)

- We try to anticipate problems.
- We discuss likely access issues in an entrance conference (e. g., PII, PHI).
- We work with agencies on strategies for resolving these matters before access battles create delays in fieldwork.

Recalcitrance and Escalation (cont'd.)

- In most cases, working with agency staff resolves these problems.
- Examples of resolution strategies include use of blinded data, MOUs, and, in some cases, we establish that there is no conflict.

Recalcitrance and Escalation (cont'd.)

- Not all endings are peaceful.
- Escalation, if used, is the responsibility of the Executive Director with assistance from the General Counsel.
- Project managers do not have the authority to escalate.
- The Executive Director may consider a meeting with the agency director to discuss the matter.
- At such meeting(s) the PEER subpoena power may be discussed.

Recalcitrance and Escalation, Final Thoughts

- Thoughtful consideration of project needs and agency prerogatives should occur before the use of subpoenas.
- You may subpoena files, records, and persons.
- Practically speaking, cooperation cannot be subpoenaed.
- Friendly subpoenas are sometimes issued, but rarely.
- When you have 100 banker's boxes of subpoenaed information, the agency is not likely to help you understand it.

The Passive-Aggressive Agency

- This problem arises from time to time.
- Consider ways to work around the passive aggressive staff.
- Methods include using in-house staff with knowledge of agency records as well as using staff in other agencies to assist.
- Discussions with the employee's director can also help.

Staff Training and Information Access

- Our analyst training package informs new staff of our access privileges.
- Staff are encouraged to discuss access problems with the General Counsel.
- Staff are taught that resolution of these problems is ultimately a matter for upper management to review and consider before action is taken.

Common Strategies, MOUs

- We often use MOUs when dealing with PHI and PII.
- Generally, this provides a quick resolution of the problem.
- Staff must ensure that MOU compliance does not create problems for the report release.
- We build a requirement in MOUs that an agency must set out in detail a PII/PHI objection and a regulatory basis for an objection when reviewing any draft.

Common Strategies; Redacted Data

- This is often helpful.
- I do not want our staff collecting and retaining certain information such as SSNs and encourage redaction of this type of information.
- Usually redaction deals with identifiers.
- Merits of redaction should be discussed in management meetings.

Other Matters

- Sometimes a “New Strategy” presents itself.
- Be open to the unique circumstances arising in each project.

Questions?
Contact
brenda.erickson@ncsl.org



NATIONAL CONFERENCE *of* STATE LEGISLATURES