



Information Technology Executive Council

Regular Meeting of the ITEC Board March 5, 2019 Minutes

The Regular Meeting of the ITEC Board was held on March 5, 2019 in the Eisenhower Room located at 2722 SW Topeka Blvd. This meeting was properly noticed and posted in the Kansas Public Square prior to the meeting.
<https://publicsquare.ks.gov/>.

Board Members:

Present unless otherwise noted

Lee Allen, Executive Branch CITO & Chairman **Absent**
Kelly O'Brien, Judicial Branch CITO
Tom Day, Legislative Branch CITO
Larry Alley, Senate Ways & Member #1
Tom Hawk, Senate Ways & Means Member #2 **Absent**
Emil Bergquist, House Govt Tech & Security Committee #1
Jeff Pittman House Govt Tech & Security Committee #2
Greg Gann, County Representative
Judy Corzine, Private Sector Representative

Nolan Jones, INK Network Manager **-Absent** (Duncan Friend attended)
Steve Funk, Board of Regents IT Director
David Marshall, KCJIS
Duane Goossen Cabinet Agency Head #1
Lee Norman, Cabinet Agency Head #2
Erik Wisner, Non-Cabinet Agency Head #1
Alexandra Blasi, Non-Cabinet Agency Head #2
Mike Mayta, City Representative **Absent**
Eric Davis, CITA (Non-voting) Board Secretary

THIS MEETING IS IN COMPLIANCE WITH
SENATE BILL 56 THAT AMENDED K.S.A. 75-7202.

Public attendees, that signed in.

Shelly Bartron, OITS
Jeff Maxon, OITS
Alan Weis, Leg IT
Sara Spinks, OITS

Duncan Friend, INK
James Weatherman, DOC ITSC Chair
Various others via the telephone

OPENING CEREMONIES – CHAIRMAN COMMENTS: Kelly O'Brien

Absent: Lee Allen, Mike Mayta, Tom Hawk, Nolan Jones

Kelly O'Brien introduced our new CITA, Eric Davis. Eric provided a brief overview of his background and what the CITA role does.

APPROVAL OF AGENDA

Motioned to Approve the Agenda by Tom Day & 2nd by Emil Bergquist.

APPROVAL OF MINUTES

Motioned to Approve the December 11, 2018 minutes by Tom Day 2nd by Eric Wisner

PRESENTATIONS - DISCUSSION AND POSSIBLE ACTION

Policy 1500: Software: Eric Davis confirmed that the ITEC policies pertain to all branches of government. The statute needs changed to make the necessary technical amendments to this policy. Suggested policy updates below:

1. 4.1 K.S.A. **2018 Supp.** 75-7203 authorizes the Information Technology Executive Council (ITEC) to adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state agencies. (Add '2018' Supp to K.S.A.)
 2. 4.2 K.S.A. **2018 Supp.** 45-221(a)(16) Public records not required to be disclosed. (Add missing 'a' to statute number.)
 3. 4.3 "An Intellectual Property Law Primer for Multimedia and Web Developers" Copyright 1996 by J. Dianne Brinson and Mark F. Radcliffe (<http://www.eff.org/pub/CAF/law/ip-primer>). (This is a dead link to a 20-year old document. Suggestion was made to remove this reference entirely.)
- Representative Pittman motioned to approve the changes to this policy, 2nd by Tom Day. -Motion passed.

ITEC Statute: 75-7202: During the 2019 legislative year, the House Government Technology & Security committee was abolished. The successor committee is the House General Government Budget Committee. The ITEC Board statute states two members from the HGTS committee are to be nominated to the ITEC Board by the speaker of the House and House minority leader. Tom day stated that we can go by the House rules and use the Successor committee this year.

-Representative Pittman motioned to have 75-7202 statute changed to remove the committee requirements for the House appointments however still be from the speaker and minority leader. 2nd by Emil Bergquist. -Motion passed. **Action Item 1: OITS Legislative Liaison (Courtney Fitzgerald) will work with Rep. Pittman to draft and present proposed legislation for ITEC board House of Representatives seats.**

ITEC Security Policy 7230a:

In December, the Information Technology Security Council, an ITEC Subcommittee, presented changes to ITEC Policy 7230a. ITEC board members asked for additional changes to the security policy. John Godfrey explained the suggested changes were made and stood for questions.

There was a lot of discussion regarding the changes.

1. Portable Electronic media policy: Brought over as much language as possible.
2. 11.4 brought over, 11.6 was in the policy before but brought up. All other ITEC policy was brought over.
3. Definition added about electronic media.
4. Question: What was the relevance between the words must and shall within the policy? Shall is less clear. The council standardized the word must to be clearer throughout the entire policy.
5. Definition of User: Definitions have been alphabetized.
6. 9 Portable Electronic, 5.16 definition of user.
7. 9.13 requirements of physical tokens. Concern at ITAB was software-based tokens. Add soft tokens can be used in addition to physical tokens. Question: Are soft tokens defined?
8. 16.0 Were there any changes made to datacenters? No changes were made except the word 'must.'
9. Representative Pittman asked if our Datacenters are required to be located in Kansas? He would like our policies to require that our datacenters be within the Continental United States.
 - A. KCJIS policy states servers must reside inside the United States. Federal Regulatory such as ITAR require datacenters must be within the US. David Marshall will locate the KCJIS rules and send to Sara Spinks (**Action Item #2**)
 - B. Greg Gann will provide Sara Spinks with a copy of Sedgwick County's data being kept inside the US rules. (**Action Item #3**)
 - C. Sara Spinks will verify with OITS Contract & Vendor manager, Angela Wilson that our contracts state that data must be kept within the United states (**Action Item #4**)

- D. Sara Spinks will collect these rules and distribute to the Board (Action Item #5)
- E. Motion made to prioritize that we explore what the language for consideration would look like to require datacenters to be located within the United states. 2nd by Greg Gann. All in favor, Motion passed. (Action Item #6)-

10. Further Discussion regarding Datacenters housing Kansas data outside the US:

Question: Do we know how many data centers that house Kansas records/data that are outside the US?
How do we call back those that already have data outside the US?

Some big companies have datacenters worldwide. Unless it is specifically spelled out in the contract that records/data must stay within the US, data could be in other countries. Representative Pittman requests that we find out what the cost would be to call it back. Also, contracts need to be clear whether our data is supported or stored outside the US. When call support is needed outside of normal business hours, you will get someone outside the country.

Greg Gann asked for a resolution to be made by the security council and encouraged the council to consider the risks when making a business case. (Action Item #7)

11. Annual Training Discussion

Kelly O'Brien asked if there was discussion at the last meeting regarding how difficult it is for some of their professional staff to take their training in a timely manner? He also asked about court staff IT equipment being a county expenditure where we have no control and no hybrid in place. Jeff Maxon stated that if they are accessing KS Info an MOU is needed stating that they will take our training.

Tom Day asked if the 8.2 Awareness & Training Standard Annual requirement is based on their anniversary or what? By Dec 31 after their initial new hire training.

Greg Gann added that at Sedgwick County he negotiates with staff to determine the best time to require training be complete. He just requires that staff take training each calendar year.

John Godfrey added that their staff is required to take security training within 90 days of hire and then must be done in September each year.

Jeff Maxon stated that the policy is written to be flexible to how each agency wants to do their training.

12. Responsibilities 19.3: Verifiable compliance within 3 months of effective date.

Eric Wisner raised a concern/caution that Small agencies may want to ensure OITS Professional Services can handle the demand of helping them determine their compliance within 3 months since they were already short staffed. OITS professional services handles their IT related needs and would be contacted to do the compliance review as well. He wondered if the policy compliance date should push out 6 or 9 months to give OITS time to broadly communicate the policy and give OITS time to incorporate all small agencies in their compliance plan. Small agency managers would depend solely on OITS/Security professionals to determine whether they meet the requirement and they want to ensure OITS can handle the task. They asked how to determine what degree they are already in compliance. The effective date was discussed whether it gives enough of a runway to comply.

Board members feel that there needs to be better communication regarding this policy by OITS. Jeff explained that the policy is not an OITS policy it is an ITEC policy that is governed by the Security Council which is an advisory council to the ITEC board. He also stated that members of the Information Security Council are aware and should have been taking this information back to their respective agencies for action. This should not be a new concept.

Some agencies may have a difficult time complying with the policy due to funding for necessary software. Eric Wisner said if OITS can meet the deadline, he is fine with the compliance date. Jeff Maxon says they are trying keep agencies from being noncompliant during Audits. Small agencies do not have the expertise within the agency and need OITS to take care of their needs.

Representative Pittman stated that agencies shouldn't be using Legislative Post Audit (LPA) as an effective mechanism for complying as their audits are usually not broad enough to be all encompassing.

Judy Corzine stated that we cannot keep pushing the date and allowing our data to be at risk. We need to start somewhere. We need a policy in place. Once adopted it becomes a standard.

Question was asked if an attorney has reviewed this policy? Answer was no.

Judy motioned to proceed to approve the 7230a policy as written It was 2nd by: Greg Gann. All in favor except Representative Pittman. -Motion passed. The policy will go into effect by Sept 2019.

Additional discussion regarding the compliance of the security policy was focused on the variance/exception template so agencies know what type of information is needed for any potential future audit.

Question was asked if anyone will be monitoring compliance? Is there some type of Metric to report each quarter to see who has met these requirements since the Focus is on compliance?

What happens at the end of Sept when a lot of groups are out of compliance?

Agencies say OITS needs to provide a variance template at the next meeting. Jeff Maxon stated the template is already on the ITEC/ITSC website.

NOTE: The exception form can be located here: <https://oits.ks.gov/docs/default-source/securitydocumentlibrary/kiso-compliancedocuments/blank-exception-form.pdf?sfvrsn=2>

Rescinding Policy 7305 due to incorporating within 7230a.

-Motion was made to eliminate Policy 7305 due to incorporating into to Policy 7230a by Representative Pittman & 2nd by Eric Wisner. Motion Passed.

David Marshall will check if KCJIS has any camera requirements. The Security council was advised by KBI when developing the policy. (Action Item 8)

More discussion took place regarding Security Policy 7230a.

The board would like a review of the status of the new policy at the next board meeting. Lee will be asked to have staff provide an update.

More discussion on the need to broadcast these changes better.

Tom Day motioned to rescind the 7230a policy approval, & there was a 2nd by Representative Pittman.

Judy Corzine added that we do not want Kansas to be in the news with security breaches. There is a current policy in place that we are attempting to update that gives us a standard to achieve.

-Motion to rescind the newly approved 7230a policy Did Not Pass.

-Motion to approve revised 7230a passed.

The board would like to see implementation guidance from OITS/IT Security Council on steps to ensure Security compliance. (Action Item #9)

KISO OFFICE UPDATE (Kansas Information Security Office)

Jeff Maxon: Security Awareness:

Last year OITS did a baseline phishing campaign which had a 19% click rate. This year the KISO did another phishing campaign with better results. If staff clicked on the phishing attempt link, the system automatically takes them to training so they learn from their mistake. KISO can also track the training and send a follow-up email.

Board Members that are managers of agencies would like to know when this happens especially those that are repeat offenders. Jeff explained that if agencies ask, the KISO will supply stats for their agency.

These phishing campaigns will become more frequent.

4% are repeat offenders.

If board members want their agency phishing exercise stats, please contact Jeff Maxon. (Action Item 10)

Jeff was asked about the exception/variance form. He stated that the Exception variance form/template is on the KISO website. Implementation guidance is being pushed. Goes to our security contacts. Pittman says extra funding is not being approved across agencies. Jeff explained it is the agency that is responsible for their compliance.

Full MFA Quote:

The board asked OITS for a multi-factor authentication quote that would include all of EBIT during the December meeting. The current quote ranges from \$600K to \$1.2 million upfront and then a yearly maintenance cost that varies depending on the solution chosen. This quote was for a mix (soft tokens, etc.)

STAFF REPORTS - DISCUSSION AND POSSIBLE ACTION

CITA role can be found in Statute 75-7204

Will there be an assessment across agencies for consolidation? Is there a Baseline for the consolidation to determine gaps between now and the future state? Eric Davis answered that this will be reviewed on a service by service basis.

COMMENTS FROM BOARD MEMBERS

None

COMMENTS FROM THE FLOOR BY THE PUBLIC

John thanked everyone for their time and discussion to get the security policy updated and passed.

CLOSING REMARKS

The board gives their condolences to Lee Allen for the passing of his mother Nova Allen.

ADJOURNMENT

Adjourned at 3:19p.m.

ACTION ITEMS

1. Action Item #1 OITS Legislative Liaison (Courtney Fitzgerald) will work with Representative Pittman to draft and present proposed legislation for statutes regarding House membership changes.

2. Action Item #2 David Marshall will locate the KCJIS rules regarding data staying within the US and provide to Sara Spinks.
3. Action Item #3 Greg Gann will provide Sara Spinks with Sedgwick County's 'keeping data inside the US' rules.
4. Action Item #4 Sara Spinks will contact Angela Wilson the OITS Contracts and Vendor manager to obtain any verbiage for keeping data inside the US. NOTE: We do have a disclaimer on our contracts regarding data staying within the US.
5. Action Item #5 Sara Spinks will collect and distribute 'keeping our data within the US rules' to the board.
6. Action Item #6 for Security Council: Motion made to prioritize that we explore what the language for consideration would look like to have the datacenters be required to be located within the United states. 2nd by Greg Gann. All in favor, Motion passed.
7. Action Item #7 Greg Gann asked for a resolution to be made by the security council and encouraged the council to consider the risks when making a business case.
8. Action Item 8 David Marshall will check if KCJIS has any camera requirements. The Security council was advised by KBI when developing the policy.
9. Action Item #9 The board would like to see implementation guidance from OITS/Security Council on steps to ensure Security policy 7230 compliance.
10. Action Item #10 If board members want their agency Security Phishing stats, please contact Jeff Maxon.

NOTE: Any individual with a disability may request accommodation in order to participate in committee meetings. Requests for accommodation should be made at least 5 working days in advance of the meeting.

ITEC BOARD MEMBERS



Lee Allen, Chairman
Executive Branch CITO



Kelly O'Brien
Judicial Branch CITO



Tom Day
Legislative Branch CITO



Steve Funk
Board of Regents IT Director



Senator Larry Alley
Senate Ways & Means



Senator Tom Hawk
Senate Ways & Means



Representative Emil Bergquist
House Govt Tech & Security



Representative Jeff Pittman
House Govt Tech & Security



Lee Norman, Secretary
Dept of Health & Environment



Duane Goossen, Secretary
Division of Administration



Erik Wisner
Real Estate Commission



Alexandra Blasi
Board of Pharmacy



Mike Mayta
City of Wichita



Nolan Jones, Manager
INK Network



David Marshall
KS Criminal Justice



Greg Gann
Sedgwick County



Judy Corzine
Private Sector Representative



Eric Davis
CITA/CTO, Board Secretary (Non-Voting)