Information Technology Executive Council

Regular Meeting of the ITEC Board
December 11, 2018
Minutes

The Regular Meeting of the ITEC Board was held on December 11, 2018 in Rm 582-N in the Kansas State Capitol, located at 300 S.W. 10th St., Topeka, KS 66612. 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
Kelly O'Brien, Judicial Branch CITO **(absent)**
Tom Day, Legislative Branch CITO
Rick Billinger, Senate Ways & Member #1 **(absent)**
Tom Hawk, Senate Ways & Means Member #2
Emil Bergquist, House Govt Tech & Security Cmte #1
Jeff Pittman House Govt Tech & Security Cmte #2 **(absent)**
Greg Gann, County Representative
Judy Corzine, Private Sector Representative

Nolan Jones, INK Network Manager
Steve Funk, Board of Regents IT Director
David Marshall, KCJIS
Sam Williams, KDOR, Cabinet Agency Head #1
Sarah Shipman, Dept of Admin, Cabinet Agency Head #2
Erik Wisner, Non-Cabinet Agency Head #1
Alexandra Blasi, Non-Cabinet Agency Head #2
Mike Mayta, City Representative **(via phone)**
Vacant, 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.

Cole Robison, OITS
Rod Blunt, OITS
John Godfrey, KUMC
Adrian Guerrero, BON
James Weatherman, KDOC
James Adams, KIC
Terri Clark, KLDIS
Katrin Osterhaus, LPA
Shelly Bartron, OITS
Courtney Fitzgerald, OITS
Sara Spinks, OITS
Unknown - via conference call

OPENING CEREMONIES

Lee Allen called the meeting to order at 1:31 pm
Lee Allen welcomed new board member Judy Corzine.

CHAIRMAN COMMENTS

None

APPROVAL OF AGENDA

Agenda Approved

Motion to approve agenda by Greg Gann, 2nd by Tom Hawk
No opposed

APPROVAL OF MINUTES

September 18, 2018 minutes were approved.
Motion to approve by Representative Bergquist, 2nd by Greg Gann
No opposed

PRESENTATIONS - DISCUSSION AND POSSIBLE ACTION

1. ITEC Policy 1210 Presenter: Cole Robison, State Director of IT Accessibility
   Action Taken: Policy Update Approved
   Motioned by Senator Tom Hawk & 2nd by Greg Gann to approve policy update.
   No opposed.

   Cole provided a brief summary of policy 1210. He proposed that Kansas IT policies align with the federal and industry standards. The update will expand policy to include all of IT, not just web applications. Any additional costs will be minimal. Vendors that follow federal standards will already comply with the updated policy. Cole provided a copy of the updated policy at the last ITEC meeting and again at this meeting.

2. ITEC Policy 7230 and Policy 7230a - John Godfrey, KU was available for questions
   James Weatherman, Chairperson of the Information Technology Security Council (ITSC) also in attendance.
   Action Taken: Policies 7220 & 4210 & 7310 Rescinded
   Motion by Senator Hawk & 2nd by Sam Williams to rescind Policies 7220 & 4210 & 7310 effective 30 days from today.
   No opposed.

   The security council requested that the board adopt the changes shown in the documents provided. These changes were requested to convert Kansas IT to a risk-driven approach rather than a response-driven approach.
   - Password requirements and multi-factor authentication requirements were updated.
   - Logging edits for incidents and change control were updated in the response section. Periodic testing requirement that meets the objectives of functional testing would be a more practical approach.
   - Section 8.2 Security Training scope includes anyone that has an account in an IT system. Sub-contractors would need annual training. Other parts of the policy lists state employees, agents and sub-contractors within the state. **ACTION ITEM: Rod Blunt will request that the Security Council define the word 'employee.'**
   - The question was asked how agencies will meet the training requirement. Rod indicated there is free Information Security Training available through the KISO as directed by statute. Additional resources for development of an agency Risk Assessment are currently provided on the KISO website.
   - Difference of opinions during the Security Council meeting consisted of password length, password change frequency and multi-factor authentication (MFA). There was a lot of discussion about extra burdens being placed on users within the agencies. The Security standards committee released some new recommendations recently on how to move forward to protect our data without causing users extra steps. The ITSC sub-committee is trying to better position state IT, so the current threats don't take advantage.

- There is a concern among the regents regarding how we make these changes happen in a timely manner. They agree that this policy advances the state and does good things; however, the compliance date seems to be too soon. What mechanism is in place to help agencies implement this policy faster? Who oversees agencies to ensure they comply? Rod Blunt, CISO explained that agencies are ultimately responsible for their data. The KISO office can be used as a resource to assist agencies with compliance. Variance statements can be developed within each agency stating they are aware of any non-compliant gaps within systems and that the agency is working toward compliance.
- There is a concern that if policies are adopted allowing variances it would cause problems.
- Board members feel that agencies need time to implement policies to allow for technology to catch up. Rod explained that these policies are in place to help agencies protect their data. Being out of compliance is a risk.
- There is a tool set within policy today that specifies what the security requirements are.
- Variance documents will be developed in many agencies, however the roadmap in each agency should address the need for compliance to security standards and develop more secure systems.
- January sounds aggressive. What would be a go-live date to implement policies to avoid as many variances as we can. The liability relies within each agency.
- The security team would love to select a compliance date where updated security policies come into effect, however, all agencies have different challenges to comply.
- Some small agencies are not aware of the policies nor how they would assess, request or establish a variance. How would a small agency meet the deadline?
- Most small agencies are overseen by a board where members are not located under the same roof so a variance would need to be added to their board meetings for discussion.
- The committee may consider a 6-month compliance date.
- Definitions throughout the document need to be consistent, i.e. employee vs agent
- Password phrases can also be considered John indicated that phrases may be a good option.
- There is a fear that agencies may extend the timeframe to the maximum time for password changes leaving their agency open for possible scams. Password requirements may need to be set enterprise wide to ensure we are being proactive in the fight against security threats.
- Suggestion was made to research software and vendors to get a cost for one MFA platform for the entire enterprise.
- Question was asked if there is a cost if we set a date to require agencies to comply with security standards. Who's going to pay for it and what would it would cost to do it right? Lee explained that in most cases O365 has security options that add no additional cost, i.e., MFA.
- The MFA requirement addition to policy is just for accounts possessing administrative rights, not all user accounts.
- We may need an RFI to see what the cost would be to cover the state as a whole.
- We will use our Unisys vendor to stand up a domain to update the Active Directory.
- Unfunded policies make people nervous.
- Each agency would be responsible for their own implementation.
- **ACTION ITEM: Lee will work with Angela Wilson and CIOs to possibly do an RFI to gather quotes of what an Enterprise wide MFA/Security Suite will cost. He may reach out to Universities who are in different stages of MFA, as a resource.**
- The board discussed passing Policy 7230, but after much discussion it was tabled for the March meeting. Discussion included
    - breaking the policy into smaller parts so that pieces could be passed today,
    - passing policy today but put a 3-month posting period looking for any objections,
    - whether variance reporting steps is included in the final version,

- putting a 6-month compliance timeline,
- whether there are Rules & Regs that need to be addressed if the board makes any changes.
- There are no Rules and Regs associated with Policy 7230.
- What the first steps would be to ensure compliance
- Reporting compliance outside the agency
- How will we communication the policy changes to the masses.
- Exempted Agencies i.e. KPERS

CISO OFFICE UPDATE/THREAT BRIEFING:

Rod Blunt, CISO

Rod reiterated that the Security Council belongs to ITEC board and is chaired by James Weatherman, not the KISO Office. The Security Council includes all branches of government.

A lot of work has been put into the security policy updates thus far. We hope to have updates for Policy 7230 and 7230a ready for a vote at the March ITEC meeting.

As one of the provisions of the Kansas Cybersecurity Act (KCA), the KISO is required to provide ITEC with a threat briefing. Rod provided an aggregate view of the enterprise.

The top three threats:

1. Ransomware –Delivered through multiple vectors, this is of particular concern because of the impact it could and has had on services at all levels of government. Industry and federal partners all agree that this type of malicious criminal behavior continues because the success rate for this activity remains high. It should also be noted that there is now an even more malicious use of ransomware, bad actors are using it as a disruptive measure with no intention of requesting a ransom.

2. Phishing: Phishing continues to be a significant problem as it still accounts for more than 95% of all malware infections and breaches. Bad actors are getting much more creative and are developing new strategies to trick users. All threat intelligence reports indicate that there will likely be no change in that this threat will remain the most significant to all business verticals.

3. Unintentional insider threat: The unintentional insider threat is “a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems." A simple example is an employee who, in the interest of providing citizen services, sends a document that includes sensitive or other information not intended for public release, to someone they shouldn’t have or a poorly written application that contains restricted use information. Though state organizations employ varying levels of data loss prevention technology, this remains a significant threat because almost every service the state provides includes sensitive or confidential information.

STAFF REPORTS - DISCUSSION AND POSSIBLE ACTION

No staff reports

COMMENTS FROM BOARD MEMBERS

Bergquist – great meeting

Blasi – Do we need to meet more frequently while these policies are being updated?

Lee – Should we call a special meeting? Do we want to address this? Yes, if the subcommittees are ready.

Day - Will be hard for Legislators to attend more frequent meetings.

Lee - We can address this in March

CITA Position Status – We are hiring a Chief Technical Officer (CTO) which will encompass the CITA will fill this role after 5-6 years being vacant.

COMMENTS FROM THE FLOOR BY THE PUBLIC

No comments

CLOSING REMARKS

Future Meetings will be held at 2722 S.W. Topeka Blvd, Topeka, KS (KS National Guard Armory)

For our travelers: Be sure to give your signed expense form to Shelly Bartron. Thank you.

ADJOURNMENT

3:35pm

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 Rick Billinger
Senate Ways & Means

Senator Tom Hawk
Senate Ways & Means

Representative Emil Bergquist
House Govt Tech & Security

Representative Jeff Pittman
House Govt Tech & Security

Sam Williams, Secretary
Dept of Revenue

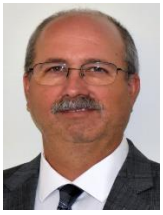
Sarah Shipman, Secretary
Dept of Administration

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

VACANT BOARD SEAT

Vacant
Private Sector Representative

Vacant
CITA/CTO, Board Secretary (Non-Voting)