


The Representative
Jim Morrison
Cybersecurity Act

March 24, 2017



HB 2331

- establishes the Kansas Information Security Office (KISO)
- affirms the office of the Chief Information Security Officer (CISO)
- establishes the cybersecurity state fund and cybersecurity state grant fund in the state treasury
- establishes the Kansas Information Technology enterprise (KITE)
- affirms the office of the Chief Information Technology Officer (CITO)*
- includes accountability and Legislative oversight measures, as well as mechanisms for KITE customers (State agencies) to address concerns and grievances

*Currently the CITO and oversight of the Office of Information Technology Services (which will become KITE) functions under the Governor's 2011 Executive Order 11-46.

Stabilize | Standardize | Secure | Sustainable

Doing What's Best for Kansas...and Kansans



Kansas Information Technology Enterprise (KITE)



Our Vision

- Financially Responsible
- Highly Performant
- Citizen/Customer-Focused



Three Pillars

- Increase Efficiency
- Improve Security
- Enhance Customer Service

Doing What's Best for Kansas...and Kansans



3

The Transformation
is Already in Motion



KITE Transformation

The transformation began in early 2016.

- Wide-Area Network (WAN).....Complete
- Office365.....Nearly Complete
- Mainframe Migration.....Implementation in Progress
- Hybrid Cloud.....In Procurement
- Statewide Mobile App.....In Procurement
- PC as a Service.....In Procurement
- V-Block Sale.....In Procurement

Doing What's Best for Kansas...and Kansans



Transformation Example: Office 365

BEFORE

- At least seven different email platforms being used across Executive Branch

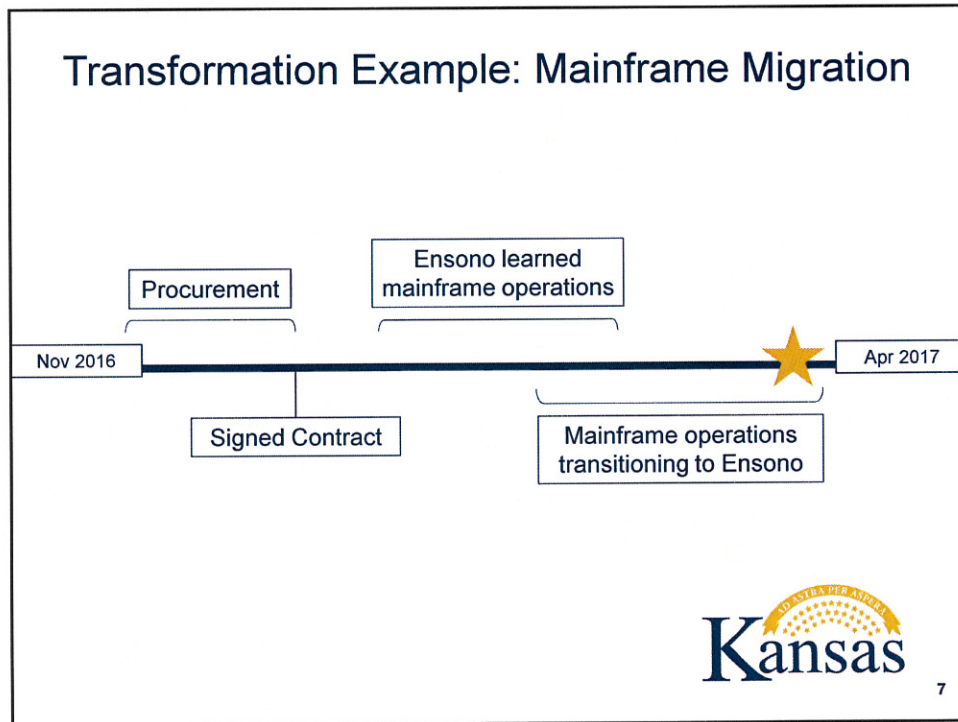
AFTER

- Consolidated vendor license
- Standardized email platform
- Increased productivity

More than 15,000 State employees now collaborating on O365.



Transformation Example: Mainframe Migration



7

KITE Transformation

A change program with eight threads.

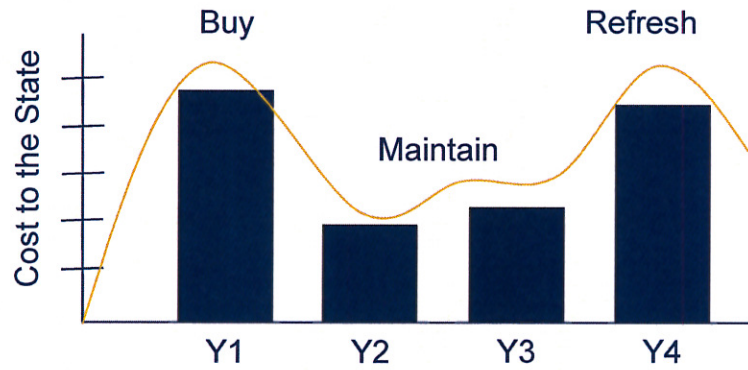
- Execution of “_____ as a Service”
- Service Management (ITIL)
- Organization
- Communications / Organizational Change
- Data Classification / Retention
- Application Lifecycle Management
- Security / Risk Management
- Finance / Funding

Doing What's Best for Kansas...and Kansans



8

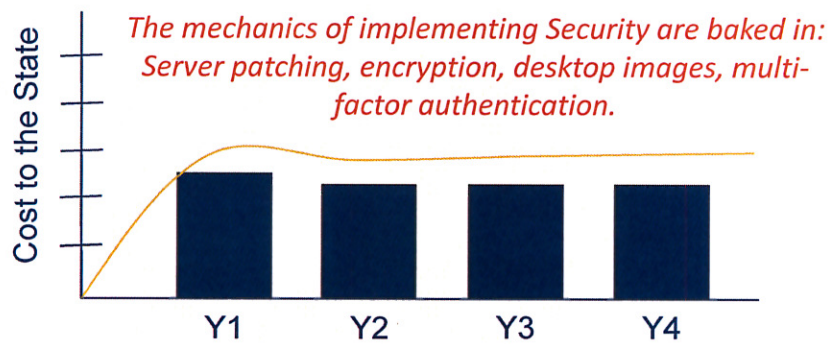
Economics of “_____ as a Service” Model



Current State



Economics of “_____ as a Service” Model



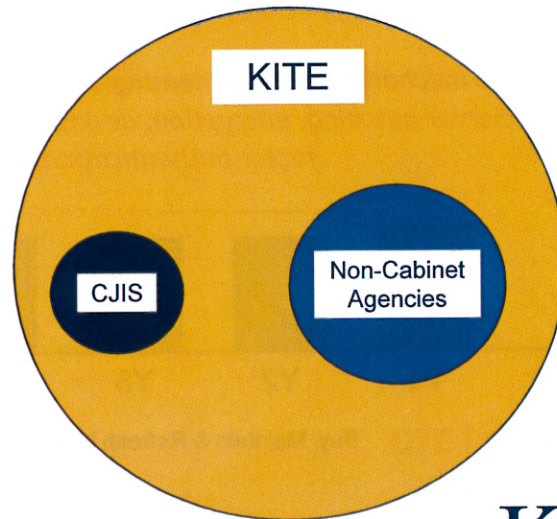
Future State Buy, Maintain & Refresh included as needed.



KITE & KISO For All Cabinet & Non-Cabinet Agencies



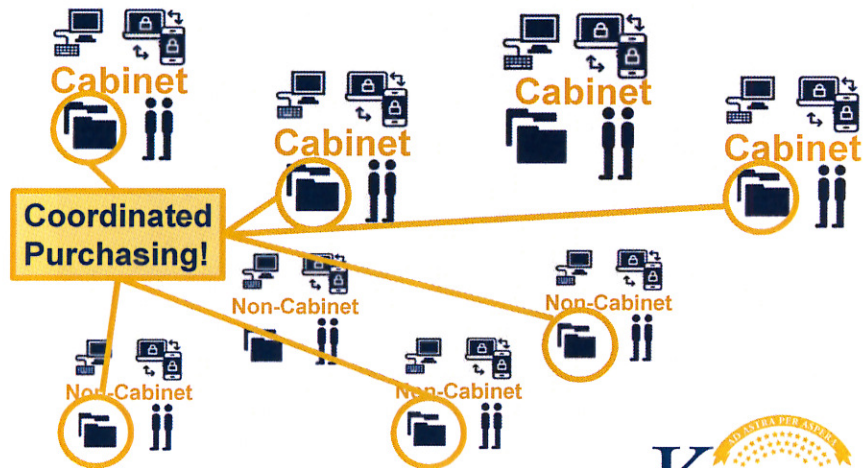
KITE: Serving Executive Branch



Doing What's Best for Kansas...and Kansans



Economies of Scale Work Best When ALL Cabinet & Non-Cabinet Agencies are Included



Doing What's Best for Kansas...and Kansans



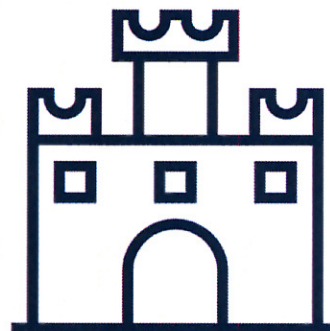
Security Only Works When ALL Accountabilities and Authorities Are Aligned

Kansas Info Security Office (KISO)

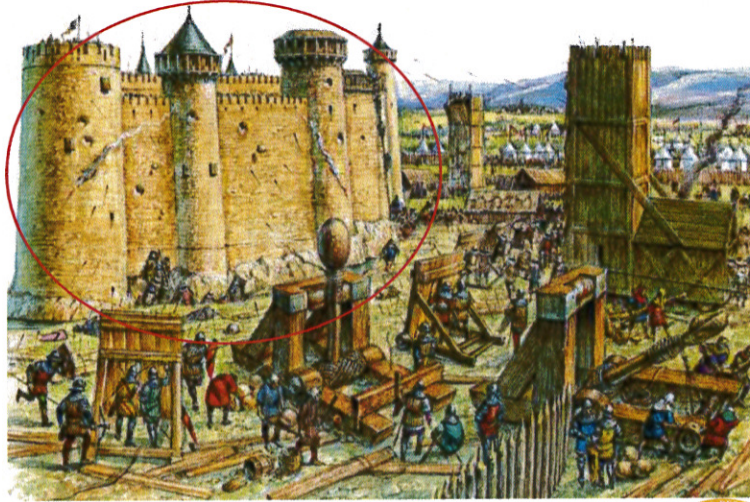
- Plans the walls, doors and moat
- Defines requirements for defending
- Tests and reports vulnerabilities
- Negotiates contracts with defenders
- Monitors defenses

Kansas IT Enterprise (KITE)

- Builds, maintains and upgrades walls, doors and moat
- Ensures all security, standards and policies are implemented and maintained as specified



Secure the Entire Castle with KITE



15

Secure the Entire Castle with KITE

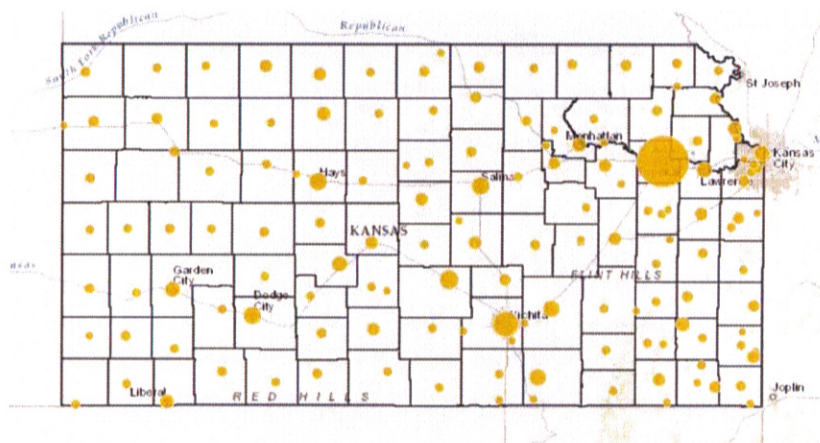


...or would you rather be these guys?



16

KanWIN: Kansas Wide Area Information Network



Kansas' private, secure computer network connecting offices across the State for the purpose of providing data, voice and internet service.



KITE & KISO

Stabilize | Standardize | Secure | Sustainable

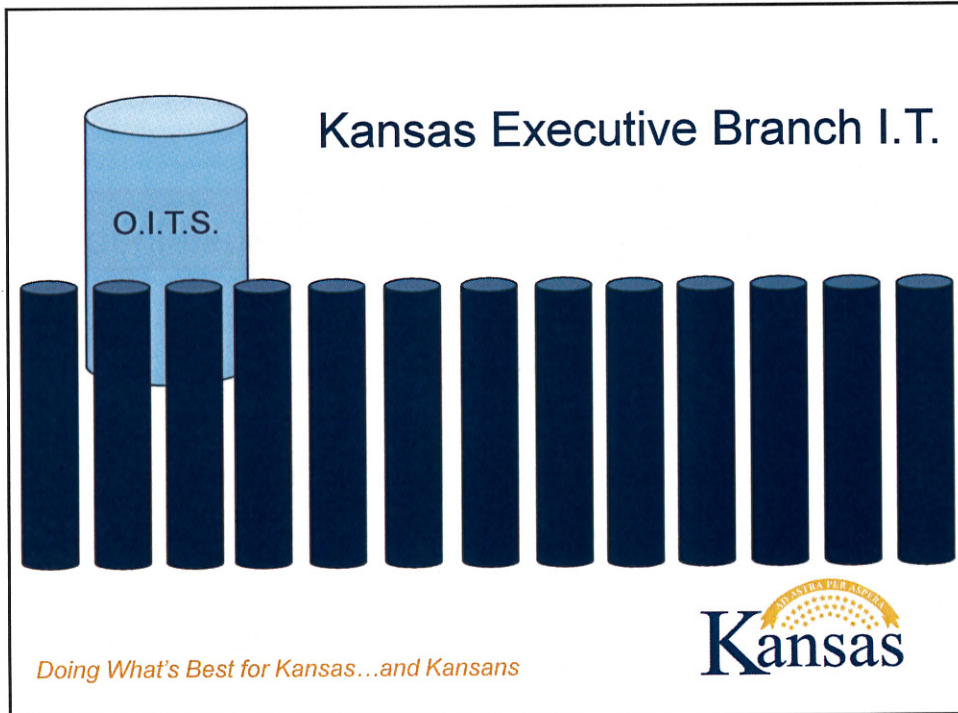
Kansas Information Technology

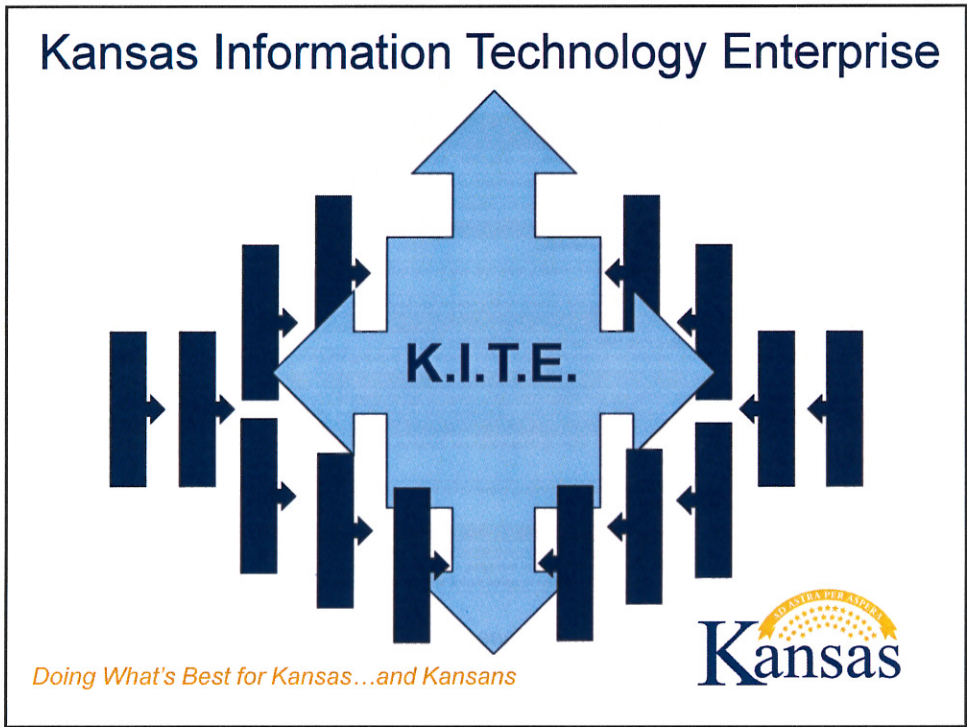
Kansas Information Security

Doing What's Best for Kansas...and Kansans



Passage of HB 2331 Leads to a More Detailed Roadmap





KITE: Planning for the Common vs Unique

Differentiating Factor	Agency 1	Agency 2	Agency 3	Agency 4	Agency 5	Agency...
Scale						
Mission Critical						
Service Levels						
Security Req's						
Risk Profile						
Funding Source						

Differentiating factors are key to designing a highly performant IT enterprise for Kansas.

Doing What's Best for Kansas...and Kansans

22

Gartner: Critical IT Processes

PROCESSES	
BUSINESS SOLUTION REQUEST	
Business Engagement	- Receives system requests/projects from business or function. Also called Account Management.
Project Prioritization	- Determining whether, when and which requested projects move forward. Involves assessing business cases and resource availability.
Approval & Funding	- Obtain client sign off, agreement to fund, if applicable, allocation of capital, agreement to fund ongoing lifecycle costs.
PROJECT EXECUTION	
Scheduling & Resourcing Projects	- IT and non-IT resource availability.
Project Management	- Client-initiated or IT-initiated. Project oversight, reporting, course correction, testing, training, go-live.
Release & Deployment Management	- Planning, scheduling and communicating release windows and accompanying outage periods.
CLIENT SERVICES	
Report System Issues	- Client requests for assistance, reporting issues, requesting new access.
Assign & Approve System Access	- End user request for system access (application, reporting), including SoX governance and other audit requirements.
CHANGE MANAGEMENT	
IT System Change Request & Approval	- Submitting and approving normal and emergency system changes (applications, infrastructure, network)
Manage Implementation & Documentation	- Executing, communicating and documenting system changes which have been approved.
INCIDENT MANAGEMENT	
Business Continuity	- The plan, including comms to clients, when significant business disruption occurs due to IT system outage. Definition is business specific but may be for outages >4 hours but <72 hours.
Disaster Recovery	- The plan, including comms to clients, when potentially catastrophic business disruption occurs to IT system. Definition is business specific, but typically if outage is expected to exceed 72 hours.
INFRASTRUCTURE & OPERATIONS	
Architecture Design Review	- Review and approval of the overall enterprise IT security architecture, including user responsibilities.
Operations	- Includes all system operations related to implementing and managing decisions of security architecture, such as server patching, firewall maintenance, 3rd party support management, and emergency actions required during security major incidents (network isolation actions).

Per "Gartner's View of IT Process Management", these are critical IT processes any organization must conduct.



KITE: Processes by Enterprise and/or Agency

Category	Process	Target A = Agency E = Enterprise
Business Solution Request	Business Engagement	A
	Project Prioritization	A / E
	Approval and Funding	A
Project Execution	Scheduling & Resourcing Projects	A
	Project Management	E / A
	Release & Deployment Management	A
Client Services	Report System Issues	E
	Assign & Approve System Access	E / A
Change Management	IT System Change Request & Approval	E
	Manage Implementation & Documentation	E
Incident Management	Business Continuity	E
	Disaster Recovery	E
Infrastructure & Operations	Architecture Design Review	E
	Operations	E

Doing What's Best for Kansas...and Kansans



Kansas Information Technology Enterprise (KITE)

Vision Statement

Collectively, as the State of Kansas' IT Leaders, we will manage the state's Information Technology capability in such a way that is:

- **Highly Performant** – *We will ensure the State's mission-critical systems and data are responsive, reliable and secure.*
- **Financially Responsible** – *We will be efficient with the State's resources, and ensure they are committed to projects and assets that deliver the most value to the people of Kansas.*

HB 2331: The Representative Jim Morrison Cybersecurity Act – FAQs

1. What is the purpose of this legislation?

The purpose of HB 2331 is to stabilize, standardize and secure information technology (IT) and information security (IS) for all Cabinet and Non-Cabinet Executive Branch agencies in the State of Kansas.

HB 2331 establishes the Kansas Information Security Office (KISO); affirms the office of the Chief Information Security Officer (CISO); establishes the cybersecurity state fund and cybersecurity state grant fund in the state treasury; establishes the Kansas Information Technology enterprise (KITE); and affirms the office of the Chief Information Technology Officer (CITO).* The bill also includes accountability and Legislative oversight measures, as well as mechanisms for KITE customers (State agencies) to address concerns and grievances.

*Currently the CITO and oversight of the Office of Information Technology Services (which will become KITE) functions under the Governor's 2011 Executive Order 11-46.

2. Why is cybersecurity important to State government?

There have been several high-profile cases in recent years where government entities were hacked and confidential citizen data was exploited by hackers. Here are just three examples:

- The U.S. Office of Personnel Management (OPM) was hacked in 2013-2014 and it's estimated more than 21 million employee records (including social security numbers and fingerprints) were exposed.
- In 2016, hackers exposed vulnerabilities in the Illinois Board of Elections, compromising up to 200,000 personal voter records. Several states, including Kansas, reported evidence of attempts from unauthorized systems to penetrate election databases.
- Millions of South Carolina Department of Revenue accounts were breached, costing the state more than \$100 million.

Of the 100 State of Kansas agencies surveyed in a 2016 Legislative Post-Audit analysis, 75 maintain some form of confidential or sensitive information about the residents of Kansas and beyond. This includes 18 agencies, which store credit card information. If any of these databases are exposed, it is projected to cost the State approximately \$200 per record in fees and monitoring. As an example, KDOR databases contain 2.7mil vehicle registration records, which include citizens' payment information. If breached, the hack could cost the State of Kansas \$540,000,000.

3. Why is it important to standardize and stabilize IT in Kansas?

The Kansas Legislature-approved Alvarez & Marsals (A&M) statewide efficiency study was only the most recent to reveal critical deficiencies in the structure, systems and operations across Kansas' IT agency siloes. Technology industry studies consistently recommend transformational change. With the approved consolidation, KITE will be able to implement best practices in IT to maximize the benefit to citizens, businesses and state agencies.

When all Cabinet and Non-Cabinet IT and IS are accountable under KITE, the State of Kansas will be able to:

- Increase cybersecurity by integrating risk and security management practices.
- Improve customer service – to internal customers (employees) and external customers (citizens and businesses).
- Provide effective, more efficient statewide operations through improved management and governance standards.
- Establish quality-driven IT performance metrics.
- Become better stewards of taxpayer dollars by leveraging economies of scale across the enterprise.
- More efficiently use human resources by institutionalizing streamlined business practices.
- Enhance the State's ability to make data-driven decisions through data analytics.
- Improve transparency by creating clear lines of accountability between agencies and KITE, as well as between KITE and the Legislature and taxpayers of Kansas.

4. What services will KITE provide to all Cabinet and Non-Cabinet Executive Branch agencies?

Under the current version of the bill (as of March 23, 2017), KITE will be able to provide **some security monitoring and maintenance** to both Cabinet and Non-Cabinet agencies.

However, to provide all needed services in the most cost-effective and security-focused manner, the bill must include ALL Cabinet and Non-Cabinet agencies.

The service KITE would ideally like to provide to all Cabinet and Non-Cabinet agencies include:

- **Security Monitoring**
- **Security Maintenance** & Upgrades
- **Risk Assessment** & Mitigation
- Data Center Operations
- Network Services
- Support Services & Help Desk
- Project Management
- Application Development & Maintenance

5. Why should all Cabinet and non-Cabinet agencies be included under KITE?

To achieve maximum security and efficiency for Kansas taxpayers and the customers of Kansas boards and commissions, it is imperative that all Cabinet and Non-Cabinet agencies remain accountable to the Legislature via KITE and KISO. The services listed in #4 are or eventually will be utilized by all agencies. Where it is possible to stabilize costs, standardize purchasing and secure systems, KITE and KISO can ensure all Executive Branch agencies are doing so.

Where there are agency-specific applications, agencies will continue to operate and maintain those systems (subject to KISO security monitoring and all applicable Legislative oversight). Examples include bridge-monitoring applications in the Kansas Department of Transportation (KDOT) and nurse licensing applications at the Kansas State Board of Nursing (KSBN).

KITE should procure, operate and maintain the infrastructure needed to support all agencies, because that is the most efficient and secure use of taxpayer and fee-payer funds. In the above example, if both KDOT and KSBN want to procure a new document imaging system, KITE can coordinate across all agencies, find out which other agencies need document imaging, leverage enterprise-wide efficiencies of scale, and ensure all agencies are paying the lowest possible price for product and service alike.

6. Why should both KITE and KISO be included in the same bill?

IT systems and process are inherently complex. Everything from phones to databases to computers to software applications are interconnected. And potentially vulnerable to attacks.

KITE and the Chief IT Officer oversee the KISO and the Chief IS Officer. This is because information security is inseparable from information technology. If the State of Kansas wants its systems and its citizens' data to be as secure as possible, KITE must have the ability (with appropriate Legislative oversight) to standardize and secure all IT systems across the enterprise.

Think of a castle. The Cybersecurity portion of HB 2331 allows Kansas to more adequately plan for and monitor the walls, moats and other fortification tools. The KITE portion of HB 2331 makes sure the walls get built, the moats stay trudded, and the fortification tools are used in a standardized, sustainable manner over time and regardless of politics or administration. If agencies are allowed to exist outside the “castle,” they cannot be assured of the most efficient and secure products and services.

7. Will this legislation result in “growing government?”

No. Executive Order 11-46 (2011) already imbues the Chief IT Officer (CITO) with authority over Executive Branch agency IT Chief Information Officers (CIOs), directors and staff performing IT functions, as well as all IT resources, functions, powers, duties, obligations, services and technology budgets vested in the State agencies/entities. HB 2331 should codify this authority into law and create the Kansas IT Enterprise (KITE) instead of the current OITS.

The Cybersecurity Act requires \$10million in annual funding. Currently the State of Kansas spends ~1% of IT funds on cybersecurity. Industry experts agree organizations should spend at least 7% of the IT budget on cybersecurity. Like all organizations – public and private sector alike – the State of Kansas must increase its investment in cybersecurity to protect its citizens’ personal and financial data.

All that said, the CITO and the CISO are already part of the Kansas Executive Branch government and this legislation simply codifies the CITO’s authorities and increases the CISO’s budget to match Kansas’ cybersecurity needs.

Executive Branch – Executive Order 11-46 Version (as written)

