FY 2012-2018 | QUARTER 2 | No. 25

The State of Oklahoma

PROGRESS ON UNIFICATION

Quarterly Report

Greetings,

Security has grown in its level of importance due to the challenge of increased cyber activities around the United States and around the globe. From attacks on a county government in the Chicago area and computers at Massachusetts Institute of Technology, to a disabled Connecticut court system, to a paid ransomware attack in Alabama, these events can be disruptive to government and the missions we accomplish.

In 2009, the Legislature passed the Oklahoma Information Services Act, mandating an assessment of all technology and telecommunication assets and services (IT Modernization Study).The study recommended establishing a statewide security operations center, consolidating agency-specific security and standardizing security tools, monitoring and infrastructure.

Armed with this information, our legislators included specific security standards as part of the Information Technology Consolidation and Coordination Act (ITCCA). The act details a need for a technology plan and enforcement of minimum mandatory standards for core technology services.

Legislators had the foresight to see technology security as a statewide responsibility. From checking voicemails and emails to updating forms on a website, technology has become a part of every business action, transaction, piece of equipment and connection.

Since 2011, OMES security has worked hard to create and provide the measures established by legislation. With the Oklahoma Cyber Command and the information security team, OMES provides these services as part of the standard service rate for 110 unified agencies and various affiliate organizations including higher education, K-12 school districts, cities and counties.

Imagine an invisible barrier that helps thwart, detect and protect. That's a great way to think of the progress of Oklahoma information security and its efforts to guard the state's most important asset: Oklahomans' data.

Another security tool is increased security awareness and reporting. I am proud to say that our security education employee program now trains over 11,000 employees annually. Employees can be not only our biggest assets, but also our biggest vulnerabilities, when dealing with cyber threats.

Risk assessment reporting has increased over the years as well. Between state agencies and higher education, we had a tremendous 94 percent participation level for the 2017 risk assessment report, up from 40 percent in 2015. We also had an average statewide compliance score of 92 percent from participating state agencies and higher education institutions.

From risk assessment reporting to cyber monitoring to employee awareness, we have dramatically improved the state's information security posture and created cybersecurity capabilities other states, federal agencies and the private sector seek to copy.

As technological innovation changes the way Oklahomans connect and conduct business, opportunities for new security vulnerabilities will continue to occur. Oklahoma had an increase of 663 percent in unique malware cyber activity from 2016 to 2017, as reported by Oklahoma Cyber Command. This reporting has now become available due to our consolidation efforts for the past six years.

While Oklahoma's technology discussion is beginning to shift to IT investments and delivering business value, our approach for security will continue to evolve to meet the challenges ahead.

We will continue to partner with Oklahoma agencies and affiliates to provide secure information technology services. We will continue working with the agencies we serve to align initiatives to better protect state employees and citizens' data.

Security is a statewide responsibility. Let's continue on our journey as technology leaders and innovators for our citizens.

Bo Reese
Chief Information Officer

TABLE OF CONTENTS

Security: A Constant Effort and Responsibility

1 Overview

Security is one of the main driving forces behind the consolidation of technology across state government. No one disputes that state governments need to be concerned with cyber risks. In Oklahoma, we have standardized and updated technology to help mitigate security risk, but as you will find, there is always more we need to do.

Security is a constant effort woven into every technology we use. While remaining in the background at all times, we highlight the security team in its constant responsibility and its accomplishments completed over the past 60 months through our IT unification efforts.

Security as a benefit through unification

In 2009, the Legislature passed the Oklahoma Information Services Act, mandating an assessment of all technology and telecommunication assets and services (IT Modernization Study).The study found:

- A large portion of State IT assets fell outside of standard warranty and support.
- Lack of unified security management.
- Significant risks due to a lack of maturity in basic processes including backup, fault tolerance and disaster recovery.

The study recommended the following changes for technology security services in state government:

- Establish a statewide security operations center.
- Consolidate agency-specific security.
- Standardize security infrastructure to two vendors at most.
- Identify tools for security monitoring.
- Identify a statewide authority for security console and reporting.

Armed with this information, our legislators included specific security standards as part of the Information Technology Consolidation and Coordination Act. The act details a need for a technology plan and enforcement of minimum mandatory standards for core technology services while also including:

- Information security and internal controls.
- Database compatibility.
- Contingency planning and disaster recovery.

Security has a part woven into all technology services and is a major benefit of unification. Since 2011, OMES security has worked hard to create and provide the measures established by the modernization study and legislation. With OMES Cyber Command and the information security team, OMES provides these services as part of the standard service rate for 110 unified agencies and various affiliate organizations including higher education, K-12 school districts, cities and counties.

In 2009, the IT Modernization study found the following:

- A lack of standardized technologies contributing to higher costs and requiring additional staffing with specialized skill sets.
- Outdated technology devices which are prone to a higher failure rate, longer recovery times and potential constraints on security.
- No centrally managed security services.
- No Security Operations Center services.
- No central patch and vulnerability management.
- No ability to uphold legal responsibility to secure FERPA/HIPAA/PCI data in use, in transit and at rest.

The IT consolidation dramatically changed our security and service posture.

What is Information Technology Security and why is it important?

The National Institute of Standards and Technology defines security as a condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems.[1]

https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

As part of the unification effort, security is a beneficial outcome of consolidated technology and provides the following benefits:

- Improved data encryption.
- Fewer IT systems hosted at insecure locations.
- Improved monitoring, detection, alerting and response capabilities.

> **"This is not a unique problem to the State of Oklahoma, it is a global issue, and we must work to identify how we meet cyber threats in the short term and long term. We need to protect not only the executive branch agencies, but every sector of our public government space."**
>
> *– Mark Gower, Former Oklahoma Chief Information Security Officer*

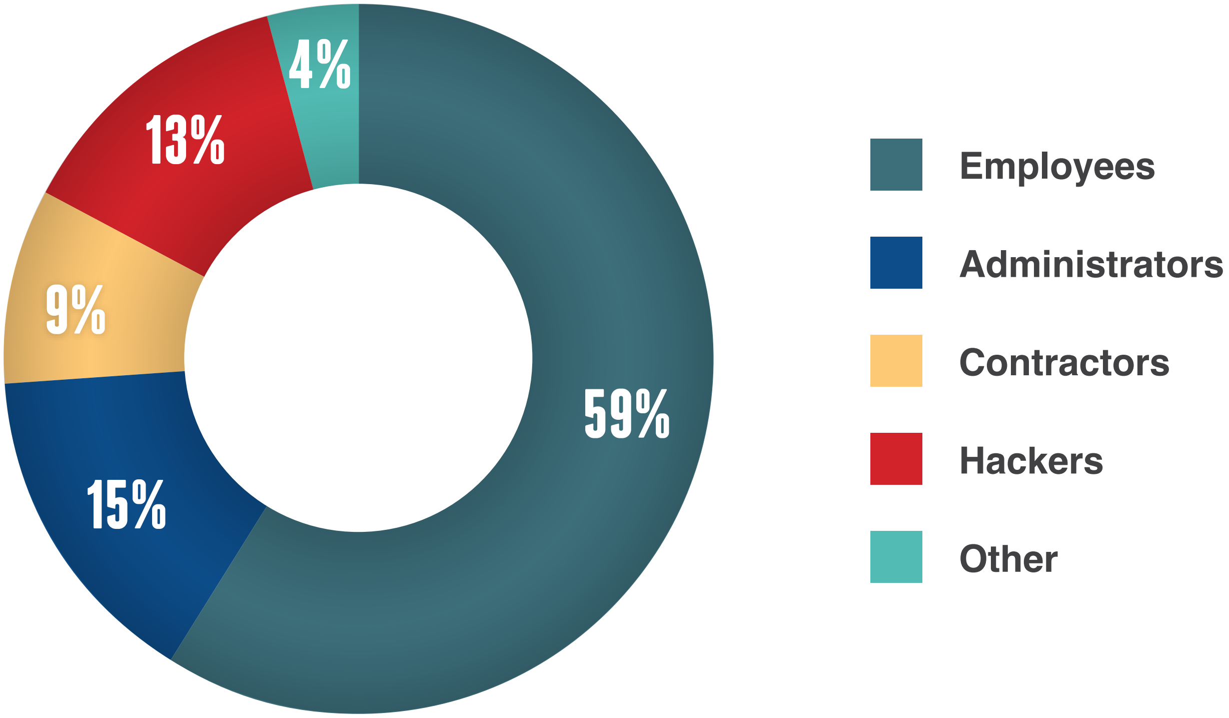
Nationally, information security has topped the list of "State CIO Top Ten Policy and Technology Priorities for 2018" for four consecutive years.[2] The top 10 mentions security and risk management in terms of governance, budget and resource requirements, security frameworks, data protection, training and awareness, insider threats and third party security practices. The cost of a data breach in the US in the public sector industry is approximately $3.6 Million, according to a 2017 study.[3]

> **Cost of a data breach in the US in the public sector industry is approximately $3.6 Million.**
>
> *– According to a 2017 study completed by the Ponemon Institute.*
>
> *2017 Ponemon Cost of Data Breach Study*

In Oklahoma, we have had an increase of 663 percent in unique malware cyber activity from 2016 to 2017, according to information now available thanks to network and monitoring consolidation efforts. Take a look at the Cyber Activity Overview chart to learn more.

Research has shown that one of the larger security risks in any organization is its employees. Employees constitute almost 60 percent of security activities, though most are inadvertent such as phishing or pharming scams from external entities. The Information Security team has instituted a security education and awareness training program to help educate about these security risks.

Users



With increased cyber activities, new regulations, changes in compliance and a need for data protection, we are encouraged to continue increasing security governance and security-enabling technologies for Oklahoma state government.

References:

1- National Institute of Standards and Technology - https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

2-State CIO Top Ten Policy and Technology Priorities for 2018 - https://www.nascio.org/topten

3-2017 Ponemon Cost of Data Breach Study - https://www.ibm.com/security/data-breach

2 Security as a Service – Centralized services

The OMES Information Security team is responsible for protecting mission-critical networks and the state's digital assets through technology, services and security best practices as well as implementing and maintaining programs that uphold the state's security posture by utilizing continual process improvement — all while providing excellent customer service. Continuous improvement efforts are in place to ensure the team is able to proactively support agency missions.

Information Security functions are organized under three general areas of work: Oklahoma Cyber Command; Unification of Central Security; and Business Continuity and Emergency Disaster Preparedness.

Additionally, the team is responsible for ensuring adherence to compliance directives by addressing issues as they arise for centralized IT as well as agency-specific services. Compliance includes all federal, state and contractual obligations as well as keeping with industry best practices. The security team facilitates onsite audits and data collection, and formally responds to all data and information requests during any audit. Any compliance and audit issues identified are then tracked and responded to by the compliance team. See table "OMES Information Security Team Milestones and Work Cycle" for more information.

Security Team Functions

The OMES Information Security Team fulfills multiple functions and roles.

General Security Support Services: Managed by OMES Security and defined as requested support services that are required by OMES IS customers.

Security Architecture and Technology Services: Oversees identity management and authentication, end point protection, server and system protection, cryptology, web filtering, intrusion detection and prevention, vulnerability management, security risk management, technical security, and maturity models.

Risk and Internal Controls Review: Defined as the management of user access, permission reviews and reporting. OMES Security develops, operates and maintains an internal user validation, permission review, and system report capacity for key information systems within the consolidated systems structure. Risk assessment services are conducted both on-demand and annually. If any contract is being modified or renewed, a risk assessment is updated to reflect OMES IS policy. As aforementioned, an online portal that provides approved and applicable risk assessments for specific systems is maintained for reference. The risk assessment control was put into place for outside vendors that OMES IS enters into contractual agreements with for any data that may be exchanged.

Security Awareness and Training Services: Provides security education and visibility to state level employees through targeted security trainings for advanced IT professionals and cyber security seminars. Additionally, OMES Security briefs new and incoming state officials on cyber security and security guidelines for traveling abroad.

Systems Development Life Cycle Management Process: In this capacity, the team oversees the System Security Development Life Cycle capacity, which provides methodology and processes to review, analyze and design for both logical and physical technical security requirements.

Security as a Service: Unified agencies receive key security services in the form of endpoint protection and cybersecurity. The Security Team also provides a core set of security services for state agencies that are not within the scope of unification, namely state affiliates. Security as a Service engages with agencies and offers services through OMES if the agency utilizes an OMES product. SaaS customers are kept up to date through a security newsletter that outlines services, security news and interests, while also receiving service product specific trainings to its customers.

Milestones/Work Cycle	
Daily	Priority case review.
Ongoing	Problem determination/root cause analysis and review, as needed.
Weekly	Review requests for changes/enhancements.
Monthly	Service quality review.
Monthly	Monthly cyber threat briefings from the MS-ISAC.
June	NASCIO – Annual Cybersecurity Survey.
July-November	State of Oklahoma – risk assessment. Annually review statewide contract for approved vendors to use for security risk assessment, report results of state agency assessments to governor, speaker of the House and president pro-tempore.
August/September	MS-ISAC – Annual Cybersecurity Risk Assessment.
August and November	Disaster Recovery Exercise – two exercises annually.
October	Annual National Cybersecurity Awareness Month (participation in numerous education and awareness events statewide).
12-month cycle of online training modules	Annual Information Security Education and Awareness Training for all state agencies, boards and commissions.
Quarterly	Every year, conduct a self-assessment questionnaire and provide a report on compliance for Payment Card Industry Data Security Standards. 100% annual requirement, conducted 25% per quarter.
Quarterly	Respond to any outstanding audit issues.
Odd years	Bi-annual DHS sponsored cyber exercise involving a joint federal task force (involves three months of planning and one week of execution).
January every three years	Every three years, coordinate a full onsite audit for the IRS Office of Safeguards for OKDHS, OTC and OESC (last one conducted in 2016).

Table 1-1: OMES Information Security Team milestones and work cycle.

Oklahoma Cyber Command and CyberWarn

Oklahoma Cyber Command was established in 2013 to help safeguard the state's data and computer infrastructure against unauthorized data use, modification, damage and loss. This initiative has provided state agencies with a uniform set of security capabilities and systems to monitor, detect and defend state systems from cyber threats.

The Security Operations Center provides centralized cybersecurity services protecting mission-critical networks 24/7/365 and monitoring over 38,000 assets. Staff respond to hackers, viruses, spam email campaigns and anything that threatens the security of the state's technology infrastructure using real-time data feeds.

SOC staff use the security tool CyberWARN for monitoring state assets. CyberWARN is comprised of intelligence feeds where correlation engines aggregate the data into a monitored visual intelligence display.

Events, attacks and incidents defined[1]

Security event: An event on a system or network detected by a security device or application.

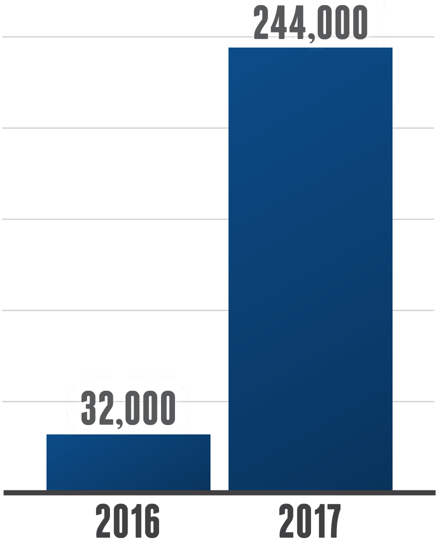
Attack: A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security incident: An attack or security event that has been reviewed by OMES security team and needs further investigation.

References:
1- National Institute of Standards and Technology - https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

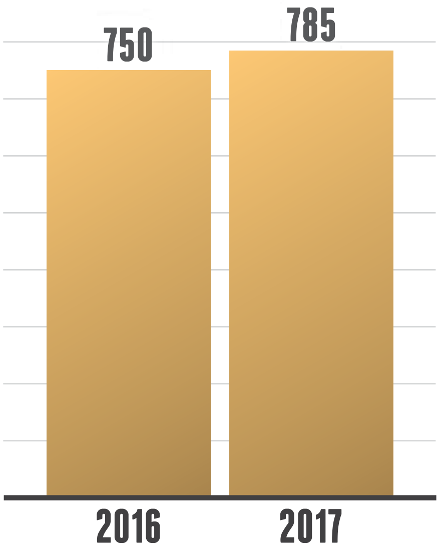
Cyber Activity Overview

Cases of Unique Malware

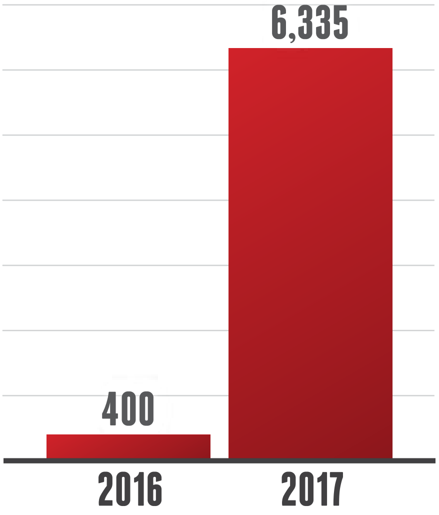


A 663 percent increase in unique malware cases from 2016 to 2017.

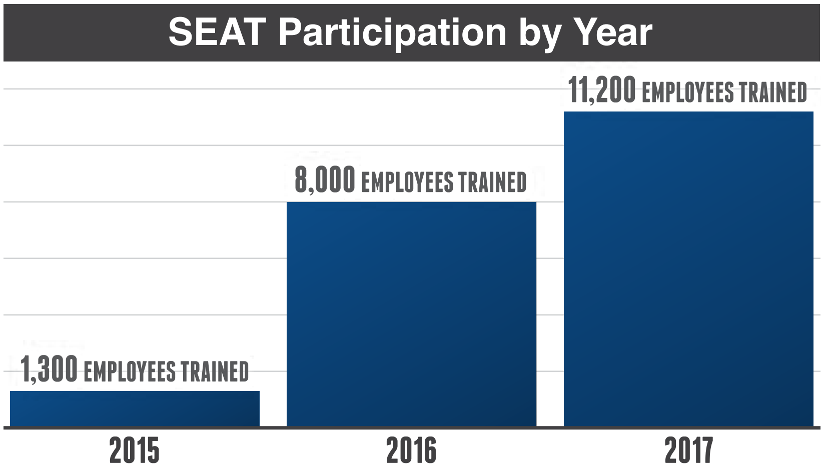
Instances of Malicious Activity



Occasions of Unauthorized Access



Security Education Awareness Training



Our workforce is our largest risk. But a workforce better educated in security awareness can make a significant difference in moving us toward a more secure work environment. Training employees is our best defense from cyber threats.

Implemented in 2014, our initiative to bring a centralized Security Education and Awareness Training, or SEAT, program to the state continues to gain success. SEAT provides online course-based training on cybersecurity, technology and regulatory topics for 12,000+ agency employees annually and counting. SEAT enables state agencies with the ability to assign training and track and report on training progress.

Business Continuity and Disaster Recovery

OMES has developed, exercised and maintained a business continuity plan for continuity of operations following a disaster. BCP includes full recovery plan exercises, planning, scheduling and onsite activities to fully exercise current recovery plans. The security team does a BCP internally for OMES, and creates BCPs for agencies, boards and commissions. Services offered to agencies include BCP training seminars, online templates and planning services. OMES Disaster Recovery planning offers oversight, management and operations that integrate through change management processes within an organization to identify DR requirements or changes. Continued maintenance through collaboration and influence occur by having a formal DR plan, procedure, exercise plan and quarterly review for a viable continuity capacity for the OMES IS data center, systems, services, and continuity requirements.

Statewide Risk Assessment Online Application

In November 2015, per Oklahoma state statute, OMES developed a standard risk assessment process to be used by all state agencies and affiliates. The annual risk assessment methodology is based on industry standards to measure the maturity of business and IT controls as it relates to information security.

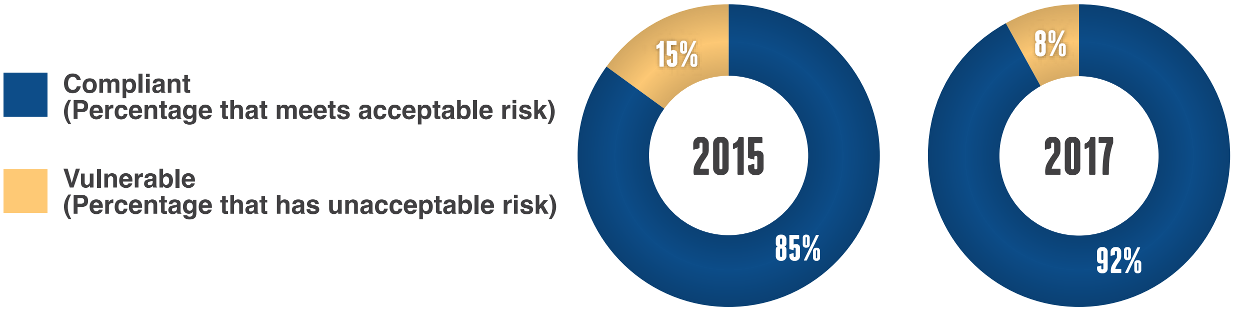
Statewide Risk Assessment accomplished the following:

- Established a baseline from which the state can measure security improvements and progress.
- Created transparency in state agency information technology and business practices to identify and report levels of acceptable and unacceptable risk.
- Identified areas of weakness where state agencies and Higher Education can improve their security posture.
- Identified the need for state resources to assist agencies not able to afford qualified security personnel or to contract for services for independent security reviews.
- Validated the need to continue and expand a state Security Education and Awareness Training Program.

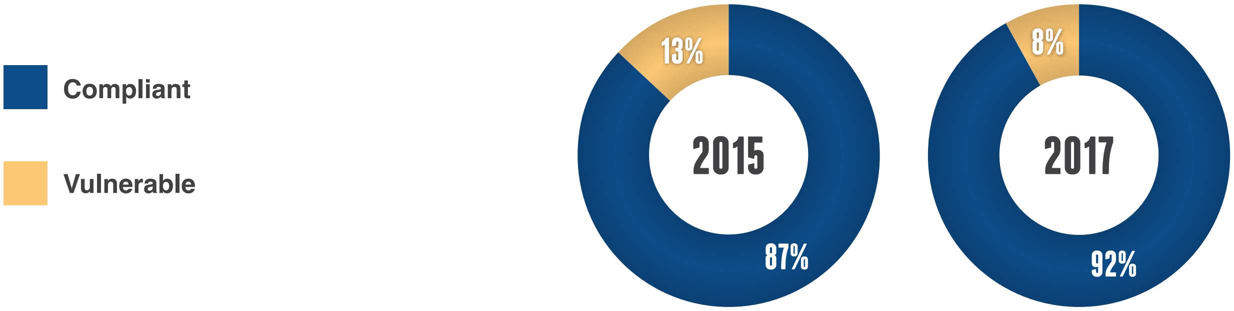
OMES created an online platform in 2015 and continues to update the platform year after year for agencies and Higher Education use. Updates include historic data of past submissions, as well as the functionality to save the survey in order to complete it at a later date and time. Thanks to this platform, the Statewide Risk Assessment survey completion rate went from 40 percent in 2015 to 94 percent in 2017.

Risk Assessment Stats Participation by Year

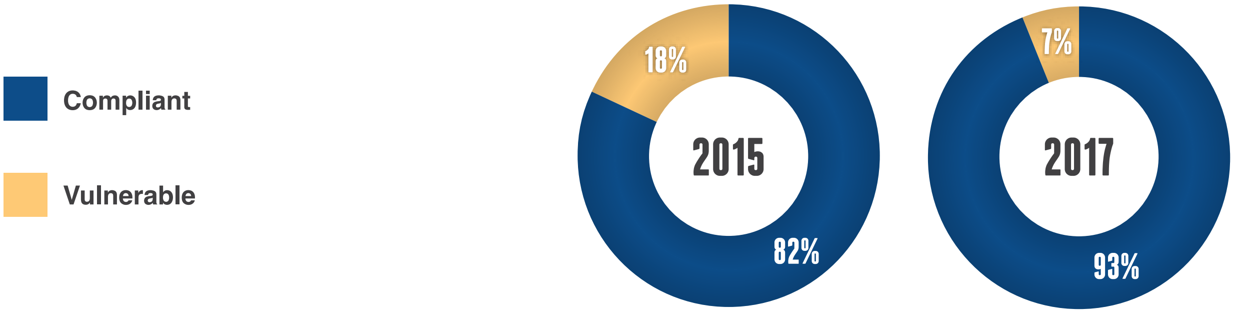
Average Statewide Compliance Score



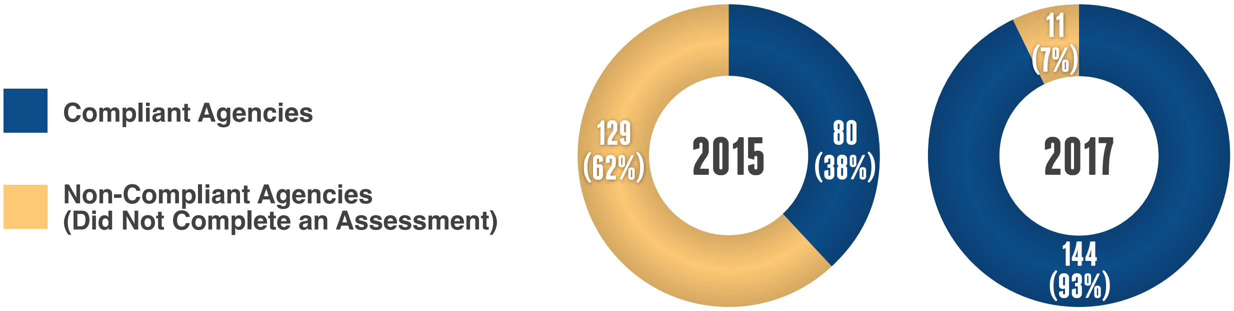
Average Agency Compliance Score



Average Higher Ed Compliance Score



Number of Agencies Completing an Assessment*



IT Audit and Compliance

The OMES Security team addresses compliance issues for centralized IT as well as agency-specific services. Compliance includes all federal, state and contractual obligations as well as keeping with industry best practices. The OMES Security team facilitates all onsite audits and data collection and formally responds to all data and information requests during any audit. Any compliance and audit issues identified are tracked and responded to by the OMES Security team.

There are many different types of federal compliance measures that agencies must adhere to in order to meet various audit and grant requirements. Sometimes these federal regulations can hinder efforts to unify states' information technology, save taxpayers' money and secure citizens' data. Oklahoma Chief Information Officer Bo Reese testified on June 21 before the U.S. Senate Homeland Security and Governmental Affairs Committee addressing these issues. View the news article "State CIO Bo Reese testifies at U.S. Senate committee" for further details.

Below are a list of some of the compliance and regulatory terms and their definitions.

Program/Grant Contractual Requirements	
Administration for Children and Families (ACF)	ACF funds state, territory, local, and tribal organizations to provide family assistance (welfare), child support, child care, Head Start, child welfare, and other programs relating to children and families.
Automated Data Processing (ADP) Rules	The Food and Nutrition Service is adopting as a final rule, without substantive changes, the proposed rule that amends the Supplemental Nutrition Assistance Program regulations to implement Section 4121 of the Food, Conservation and Energy Act of 2008 (the Farm Bill), which requires adequate system testing before and after implementation of a new state automated data processing and information retrieval system, including the evaluation of data from pilot projects in limited areas for major systems changes, before the secretary approves the system to be implemented more broadly.
Centers for Medicare and Medicaid Services (CMS)	CMS is a federal agency within the United States Department of Health and Human Services that administers the Medicare program and works in partnership with state governments to administer Medicaid, the Children's Health Insurance Program, and health insurance portability standards.
Food and Nutrition Services (FNS)	FNS administers the nutrition assistance programs of the U.S. Department of Agriculture. The mission of FNS is to provide children and needy families better access to food and a more healthful diet through its food assistance programs and comprehensive nutrition education efforts.
Department of Defense (DoD, USDOD, or DOD)	The DoD is an executive branch department of the federal government of the United States charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces.
Office of Child Support Enforcement (OCSE) Data Reliability Audit (DRA)	The purpose of these audits is to assess the completeness, reliability and security of states' systems that store and process the data reported on the Child Support Enforcement Annual Data Report.

MANDATED GUIDELINES and STANDARDS (Programs, Auditors and Industry Best Practice)	
Center for Internet Security (CIS) Critical Top 20 Security Controls	CIS Prioritizes security controls for effectiveness against real world threats. CIS Top 20 Critical Security Controls (previously known as the SANS Top 20 Critical Security Controls) is a prioritized set of best practices created to stop the most pervasive and dangerous threats of today.
Committee of Sponsoring Organizations (COSO)	COSO's mission is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.
Control Objectives for Information and Related Technologies (CobiT) 4.1	CobiT is a good-practice framework created by international professional association Information Systems Audit and Control Association for information technology management and IT governance.
Information Technology Infrastructure Library (ITIL)	ITIL is a library of volumes describing a framework of best practices for delivering IT services. ITIL has gone through several revisions in its history and currently comprises five books, each covering various processes and stages of the IT service lifecycle.
National Institute of Standards and Technology (NIST) Cybersecurity Framework	This voluntary framework consists of standards, guidelines and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.
State Security Policy (SSP) – ISO 270001/270002	Created by OMES for the State of Oklahoma is a reference of best practices for IT governance. ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system. An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. ISO/IEC 27002 is an information security standard published by the International Organization for Standardization and by the International Electro-technical Commission, titled Information technology – Security techniques – Code of practice for information security controls.
Statewide Automated Child Welfare Information System (SACWIS)	SACWIS and Tribal Automated Child Welfare Information System are federally funded, voluntary, comprehensive and automated case management tools that support child welfare practice in states and tribes.
SANS Glossary of Security Terms	

Highlight: Important Technology Regulations and Compliance

We have highlighted a few of the most important technology regulations and provided effects on agencies, technology updates and an updated definition to meet this regulation.

Criminal Justice Information Systems

Established in 1992, CJIS is the largest division of the FBI, and comprises several departments, including the National Crime Information Center, Integrated Automated Fingerprint Identification System and the National Instant Criminal Background Check System. CJIS monitors criminal activities in local and international communities using analytics and statistics provided by law enforcement, and their databases provide a centralized source of criminal justice information to agencies around the country.

The proliferation of the Internet and the cloud, combined with the growing rate and sophistication of cyber security threats, have made protecting CJIS data more complicated than ever. Because of this growing concern, CJIS has security standards for organizations, cloud vendors, state agencies and corporate networks.

The policies set forth by CJIS cover best practices in the following areas:

- Information exchange agreements.
- Security awareness training.
- Incident response.
- Auditing and accountability.
- Identification and authentication.
- Configuration management.
- Media protection.
- Physical protection.

Who does CJIS affect?

- Emergency Management.
- Alcoholic Beverage Laws Enforcement (ABLE) Commission.
- Office of the State Fire Marshal.
- Department of Public Safety.
- District Attorneys Council.
- Office of the State Attorney General.
- Oklahoma State Bureau of Investigation.
- Indigent Defense System.
- Office of Homeland Security.
- Department of Corrections.
- Council on Law Enforcement Education and Training.
- Bureau of Narcotics and Dangerous Drugs.
- Office of the Chief Medical Examiner.

Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information (PII) from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student.

FERPA requires that federally funded institutions, under programs administered by the U.S. Department of Education, comply with certain procedures with regard to disclosing and maintaining educational records. FERPA classifies protected information into three categories: educational information, PII and directory information. The limitations imposed by FERPA vary with respect to each category.

A comprehensive data governance plan that outlines organizational policies and standards regarding data security and individual privacy protection should be in place. The plan should clearly identify staff responsibilities for maintaining data security and empower employees by providing tools they can use to minimize the risks of unauthorized access to PII. Best practices for protecting student information should be included in the plan, including the following:

- Access Control.
- Asset Inventory.
- Authentication (at least two-factor authentication is recommended).
- Automated Vulnerability Scanning.
- Encrypted Mobile Devices.
- Firewalls and Intrusion Detection/Prevention Systems.
- Network Mapping.
- Patch Management.
- Personnel and Physical Security.
- Secure configuration.

Who does FERPA affect?

- Department of Education.
- Department of Career and Technology Education.
- Office of Educational Quality and Accountability.

Federal Tax Info and Internal Revenue Service Publication 1075

Internal Revenue Service Publication 1075 (IRS 1075) provides guidance for US government agencies and their agents that access federal tax information (FTI) to ensure that they use policies, practices, and controls to protect its confidentiality.

FTI can include name, social security number and tax return information, as well as account numbers and benefit qualifications related to social entitlement programs. Whether information qualifies as federal PII generally depends on whether it comes from a US federal source. If PII comes from the Social Security Administration, the Department of Health and Human Services, the IRS or another federal agency, it should be assumed that it is federal PII, and is protected by federal law. Some of the controls that are needed are as follows:

- Record Keeping Requirements.
- Secure Storage.
- Restricting Access.
- Reporting Requirements.
- Training and Inspections.
- Data Disposal.
- Computer System Security.

Who does FTI affect?

- Department of Human Services.
- Employment Security Commission.
- Office of Management and Enterprise Services.
- Tax Commission.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act, or HIPAA, governs the use, transfer, and disclosure of health-related information. One of the requirements of HIPAA is the protection of protected health information, known as PHI. PHI is defined as any piece of individual health information that can identify an individual, such as a person's medical record, street address, or telephone number. Protecting PHI applies to organizations that store, process, or transfer patient information in electronic, paper, or oral form.

Established in 1996, the HIPAA regulations were updated in 2009, which included the Health Information Technology for Economic and Clinical Health Act, also known as the HITECH Act. The HITECH Act is the same law that created the Electronic Health Records Incentive Program, as well as the HIPAA Breach Notification Rule.

Safeguarding PHI is an important requirement. The Breach Notification Rule requires that Covered Entities and Business Associates must provide notification of a breach to affected individuals, the Secretary of the U.S. Department of Health & Human Services, and in certain circumstances, the media. A breach means that information obtained, accessed, used, or disclosed leads to a compromise of security or privacy of that data related to PHI.

A central principle of HIPAA is "minimum necessary use and disclosure." Reasonable efforts must be made to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

Who does HIPAA affect?

- Department of Health.
- Department of Mental Health and Substance Abuse Services.
- Department of Human Services.
- Department of Rehabilitation Services.
- Health Care Authority.
- Office of Juvenile Affairs.

Payment Card Industry Data Security Standard

PCI DSS are technical and operational requirements that protect cardholder data. Cardholder data includes the payment card number (known as a Primary Account Number, or PAN) and any associated account information, including the cardholder's name, the payment card's expiration date, the three or four-digit verification code, and any other authentication data related to the cardholder.

The standards globally govern all merchants and organizations that store, process or transmit this data. Compliance with the PCI set of standards is mandatory, and is enforced by the major payment card brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. PCI Standards Include:

PCI Data Security Standard: This standard covers technical and operational system components included in or connected to cardholder data. If an entity accepts or processes payment cards, it must comply with the PCI DSS.

PCI Data Security Standard for Merchants & Processors: This is the global data security standard that any entity of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

Who does PCI DSS affect?

Any state agency or entity that utilizes credit cards as a form of payment for goods or services.

Social Security Administration Systems Security Requirements and Electronic Information Exchange Partners

The Social Security Administration requires Electronic Information Exchange Partners to meet information security safeguards requirements, which are intended to protect SSA-provided information from unauthorized access and improper disclosure.

As a prerequisite to receiving information, SSA must certify that EIEP are in full compliance with all the management, operational, and technical aspects of safeguards, to ensure that unauthorized disclosure and usage of SSA provided information does not occur.

SSA requires EIEPs to maintain an organizational access control structure that adheres to a three-tiered best practices model. The SSA recommended model is "separation of duties," "need-to-know" and "least privilege" based on each user's position and job-related duties. SSA also recommends that each EIEP develop and publish a comprehensive Information Technology Systems Security Policy document.

Who does EIEP affect?

- Oklahoma Department of Human Services.
- Oklahoma Department of Public Safety.
- Office of Management and Enterprise Services.

> **"State CIOs and chief information security officers must comb through thousands of pages of federal regulations to ensure that states are in compliance with rules from our federal partners," he said.**
>
> *– Bo Reese, Oklahoma Chief Information Officer*

3 Increased Importance of the CISO Role

> **"Security is constantly evolving to protect against, detect, and respond to incidents that might compromise critical data or assets."**
>
> *– Mark Gower, Oklahoma Chief Information Security Officer*

The chief information security officer role is rapidly maturing from being IT-centric to becoming an integral part of a security and risk framework with access to the highest levels of the organization. According to a recent Ponemon study, 65 percent of respondents say they report to senior executives.[1] This shift makes the chief information security officer role a complex one and not easy to fill.

As the Chief Information Security Officer and Cyber Command Director, Mark Gower has been a leader both at the state and national level in enhancing state security capabilities and accessing and anticipating risk to ensure the protection of state assets.

Since 2010, NASCIO in conjunction with Deloitte, has conducted biennial surveys of the role of the CISO and state officials.[2] The survey results indicate that governors and other state officials are receiving more frequent reports from CIOs/CISOs.

CISO Gower conducts an annual risk assessment survey, disaster recovery and cyber threat annual report for Gov. Mary Fallin. These reports are critical in keeping our state officials informed. However, according to the survey, communicating the severity of cyber threats to state officials may need to be handled differently.[3]

CISOs are focusing on areas where they can take proactive steps to better manage risks. Some of the top areas CISOs say are within their arsenal to thwart, detect and protect state assets include audit logs and security event monitoring, strategy and planning and awareness and training.[4]

Since 2013, the Oklahoma Cyber Command has used a display dashboard to monitor security threats, titled as CyberWARN. CyberWARN is comprised of intelligence feeds where correlation engines aggregate the data into a monitored visual intelligence display dashboard.

Since 2014, Oklahoma has been enrolling state agency employees into an annual security education and awareness program. SEAT now trains more than 11,000 employees annually through an online course-based software on cybersecurity, technology and regulatory topics.

The role of the CISO includes not only threat detection, prevention and reporting typical of the technology role but also includes business decisions in terms of identifying risks for new products and services, staffing and budgeting and more.

The Oklahoma Cyber Command and the OMES security team were established to help protect the state's assets and data. The team has evolved to include new roles for disaster recovery planning, technology and system architecture, risk and internal controls review, security education and awareness, risk assessment and security auditing.

Effective CISOs know when to be collaborative, when to be visionary, when to listen and when to command. They have a genuine passion for their mission and that passion is contagious. Gower has effectively established the role of the CISO and will continue in his path to secure Oklahoma's most important state asset: citizen data.

References:

1-The Evolving Role of the CISOs
https://interact.f5.com/CISOResearchReport-RegistrationPage.html

2,3,4-2016 Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress
https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress

4 In the News

News Article 1 – December 2013

> **"As statewide IT consolidation has progressed, Oklahoma's ability to improve security across the entire state network has increased dramatically."**
>
> *– Mark Gower, Oklahoma Chief Information Security Officer*

Link to this article: https://content.govdelivery.com/accounts/OKOMES/bulletins/97a344

Dec. 4, 2013

OMES launches IT Security Operations Center

Oklahoma becomes national leader in state IT security

OKLAHOMA CITY — State government's computer network has been made far more secure with the launch of Oklahoma's first statewide information technology Security Operations Center.

The SOC, developed and administered by the Office of Management and Enterprise Services, provides real-time security monitoring and threat alerts for all state computers, allowing the state to thwart attacks from hackers and other information technology security risks at a far higher rate than in the past.

"We place the highest premium on keeping the taxpayers' information as secure as possible," said OMES Chief Security Officer Mark Gower. "As statewide IT consolidation has progressed, Oklahoma's ability to improve security across the entire state network has increased dramatically. The SOC, in particular, has eliminated a significant amount of vulnerability that existed previously when each agency was running its own IT services without any uniform, statewide security standards."

The SOC, launched in January and now fully operational, has made Oklahoma's information technology security posture stronger than most other state governments. As of Nov. 1, approximately 28,000 of the state's 34,000 computers are monitored by the SOC. The SOC's goal is to monitor all state computers by the end of 2015.

Symantec, a Fortune 500 company and leading information technology security provider, called Oklahoma's security model a "blueprint" for other state governments to adopt.

"In today's threat landscape, state and local governments need real-time monitoring and security intelligence to effectively protect against advanced persistent threats and targeted attacks," said Amber Johanson, senior director, Public Sector Engineering, Symantec. "By deploying a statewide Security Operations Center, the State of Oklahoma is taking the steps necessary to proactively protect their employees and residents from security risks, while also creating a blueprint for other state governments to adopt."

The SOC is designed to alert a staff of dedicated security personnel to any potential threat to a state computer or the state network. It also tracks state computer usage to ensure users are not engaging in behavior that could pose security risks.

"In today's world, all large networks face constant, daily attacks from hackers and other threats. The high level of security that Oklahoma's state government now enjoys is possible because policymakers made the wise decision to centrally consolidate state IT services," said state Chief Information Officer Alex Pettit. "Off-the-shelf security services were projected to cost up to $600,000, but we were able to build a superior solution at no additional cost using our own in-house resources. Increasing security to this level while also containing cost is a superb accomplishment that demonstrates tremendous talent and vision in the state's IT workforce."

News Article 2 – May 2017

> **“Having Oklahoma CyberCommand and other protections and redundancies in place is an important part of IT unification. Simply put, the State of Oklahoma is stronger with a unified IT infrastructure.”**
>
> *– Bo Reese, Oklahoma Chief Information Officer*

Link to this article: https://omes.ok.gov/articles/omes-it-unification-protects-state-data-attack

May 15, 2017

OMES IT unification protects state data from attack

OKLAHOMA CITY — As a ransomware cyberattack created worldwide chaos, State of Oklahoma agencies with their information technology unified under the IT umbrella managed by the Office of Management and Enterprise Services were protected and reported no disruptions in service.

Unification allows agencies to have the updated resources of Oklahoma CyberCommand that quickly detect and respond to ransomware attacks.

“CyberCommand has a specific set of technical and response capabilities to identify and respond to cyberattacks,” said Oklahoma CyberCommand Director Mark Gower. “During the latest global incident, we had zero reports of encryptions and no indicators of a compromised system due to this ransomware.”

Nonunified agencies are responsible for their own cybersecurity and typically don’t have immediate access to the updated resources available through Oklahoma CyberCommand and can therefore be more vulnerable.

“The focus of OMES to protect unified agencies against a cyberattack that brought down other systems worldwide, proves the value of IT consolidation,” said Secretary of Finance, Administration and Information Technology Preston L. Doerflinger, who is the director of OMES. “As this incident shows, misguided efforts to resist unification could lock up vital systems in a time of need or even allow the private information of Oklahomans to fall into the wrong hands.”

Ransomware is malware that installs itself on a device and holds data hostage until a ransom is paid. In 2016, CyberCommand successfully responded to about 32,000 cases of unique malware, about 750 instances of malicious activity, nearly 400 occasions of unauthorized access and two denial-of-service attacks. The state’s ongoing information technology unification efforts and the OMES Security Operations Center can identify and quickly respond 24/7 to cyberattacks.

Starting Friday with the first reports of the ransomware attack known as Wannacry, OMES activated technical teams to make sure state systems were not vulnerable and to mitigate related risks to the state’s technology infrastructure. OMES technicians’ initial focus on the systems and workstations of unified agencies transitioned to include outreach to nonunified agencies and affiliates over the weekend.

“As with past threats, this current threat and any future threat, we will always take the time to validate we have the right IT and security posture to protect the state,” Gower said. “We took the weekend to review security of systems and make any adjustments we felt necessary to help guard against threats.”

The latest ransomware attack targeted current and outdated Microsoft Operating Systems for both workstations and servers, such as Windows XP. Prior to the attack, OMES had removed Windows XP, as it went out of support in 2014, and upgraded computer systems for unified agencies. Still, technicians scanned networks, applied systems patches, updated anti-virus capabilities and made changes to networks and email systems to further protect state data.

“We wanted to make sure we were protected,” Gower said. “If you heard that burglars were in your neighborhood, you would certainly want to go and check that the windows and doors were locked.”

This is the second time in recent weeks that unplanned incidents have shown the value of unifying IT with OMES. When strong storms knocked out power at the Capitol during last weekend of April, the data of unified agencies remained secure and accessible at the OMES Data Center, where generators kicked into gear almost immediately and kept the state's data online.

"Having Oklahoma CyberCommand and other protections and redundancies in place is an important part of IT unification," said Oklahoma Chief Information Officer Bo Reese. "Simply put, the State of Oklahoma is stronger with a unified IT infrastructure."

Unification, legislatively mandated by HB 1304 in 2011, partners agencies with OMES to streamline and consolidate IT efforts. By the end of fiscal year 2017, 78 mandated agencies, and more than 30 voluntary (nonappropriated) state agencies, will have been brought under one IT umbrella at an estimated reduced spending and projected savings of about $130 million. The increased purchasing power of unification saved the state another $46 million in FY 16 in IT contracts.

News Article 3 – June 2017

June 21, 2017

State CIO Bo Reese testifies at U.S. Senate committee

Head of OMES Information Services speaks on federal cybersecurity regulations

Link to this article: https://omes.ok.gov/articles/state-cio-bo-reese-testifies-us-senate-committee

WASHINGTON — Duplicative and inconsistent federal regulations can hinder efforts to unify states' information technology, save taxpayers' money and secure citizens' data, Oklahoma Chief Information Officer Bo Reese testified today before the U.S. Senate Homeland Security and Governmental Affairs Committee.

"Over the past five years, (OMES has) reduced these redundancies, made large strides to unifying technology, and completed consolidation of 76 of the 78 mandated state agencies and more than 30 voluntary agencies," said Reese, who leads the Information Services division for the Office of Management and Enterprise Services.

"Consolidation has resulted in $283 million of estimated reduced spending and projected savings," Reese said. Oklahoma's IT unification has also created a robust cybersecurity program, Oklahoma Cyber Command. In 2016, Cyber Command successfully responded to about 32,000 cases of unique malware, about 750 instances of malicious activity and nearly 400 occasions of unauthorized access.

"We appreciate efforts by the federal government to secure and protect sensitive citizen information because we also share that responsibility at the state level," Reese said. "But, we must accomplish our shared goal without overly burdening state governments, ensuring that we are delivering government services to citizens in the most efficient and cost-effective manner."

Reese, who also serves as vice president of the National Association of State Chief Information Officers, was invited to testify at the hearing, "Cybersecurity Regulation Harmonization," to give an overview on how federal data security regulations impact the work of CIOs to introduce efficiencies and generate savings.

"State CIOs and chief information security officers must comb through thousands of pages of federal regulations to ensure that states are in compliance with rules from our federal partners," he said. "Even though many federal regulations are similar in nature, in that they aim to protect high-risk information, they are mostly duplicative but have minor differences which can obscure the goal of IT consolidation, the whole point of which is to streamline IT applications and simplify the enterprise IT environment to produce savings for taxpayers."

In his testimony, Reese brought attention to several federal cybersecurity regulations that pose obstacles for state IT unification and risk-based cybersecurity investments. Examples included differences in IRS and FBI regulations on what to include in passwords and how long to keep them.

Reese also called on federal regulatory agencies to normalize the federal cybersecurity compliance audit process which encourages states to make counterproductive compliance investments instead of ones based on risk.

"This approach is problematic for state government cybersecurity because it encourages state CIOs to make check-the-box compliance investments instead of ones based on risk, which is the more secure approach to managing sensitive data."

Reese's full testimony and a recording of the hearing can be found on the U.S. Senate Homeland Security and Governmental Affairs Committee website.

In the News

The Oklahoman Newspaper - December 1, 2013 - State cyber security operation battles hackers

http://newsok.com/state-cyber-security-operation-battles-hackers/article/3909803

Dec. 2, 2013 – Government Technology – Oklahoma Cybersecurity Operation Battles Hackers

http://www.govtech.com/security/Oklahoma-Cybersecurity-Operation-Battles-Hackers.html

The Tulsa World newspaper - via The Oklahoman - Oklahoma boasts top cybersecurity center

http://www.tulsaworld.com/content/tncms/assets/v3/eedition/5/37/53747f97-7000-5b90-9d53-f71c3bccf44e/529afbb2ceb55.pdf.pdf

NASCIO - Translating Big Data into Centralized Cybersecurity Threat Response - Cybersecurity Initiatives - Mark Gower

https://www.nascio.org/portals/0/awards/nominations2014/2014/2014OK10-OK_NASCIO_SOC.pdf

State of Oklahoma press release - December 4, 2013 - Oklahoma becomes national leader in state IT security

http://content.govdelivery.com/accounts/OKOMES/bulletins/97a344

OETA - Cyber Espionage - July 2014

http://www.okhorizon.com/shows/2014-show-archive/July%202014/Show%201430/cyber-espionage

May 01, 2015 - Oklahoma City FOX 25 News - Oklahoma cyber security operation model for country.

http://www.okcfox.com/story/28776102/oklahoma-cyber-security-operation-model-for-country

July 22, 2015 - News 9 - Keeping the State of Oklahoma Secure Against A Cyber Attack.

http://www.news9.com/story/29612199/keeping-the-state-of-oklahoma-secure-against-a-cyber-attack

September 03, 2015 - News 9 - Virus Hits Moore Public Schools Computer Systems

http://m.news9.com/Story.aspx?story=29956107&catId=112032

February 26, 2016 - The Journal Record - Keeping out the hackers: 11,000 attacks launched per week on state computers

http://journalrecord.com/tag/mark-gower/

March 1, 2017 – IT unification saves millions and enhances cybersecurity, OMES Press Release

https://omes.ok.gov/articles/it-unification-saves-millions-and-enhances-cybersecurity

May 15, 2017 - OMES IT unification protects state data from attack, OMES Press Release

https://omes.ok.gov/articles/omes-it-unification-protects-state-data-attack

June 21, 2017 - State CIO Bo Reese testifies at U.S. Senate committee, OMES Press Release

https://omes.ok.gov/articles/state-cio-bo-reese-testifies-us-senate-committee

January 19, 2018 - States push feds to 'harmonize' cybersecurity regulations in 2018

https://statescoop.com/states-push-feds-to-harmonize-cybersecurity-regulations-in-2018

5 Oklahoma IT Strategic Plan

Current technology expectations require Oklahoma government agencies to be ready to deliver and receive digital information and services anytime, anywhere and on any device. It must do so safely, securely and with fewer resources. Thus, Oklahoma has developed a digital strategy that embraces the opportunity to innovate more with less and enables entrepreneurs to better leverage government data to improve the quality of services to Oklahomans and develop a Digital Oklahoma.

The 2017-2021 IT strategic plan for Oklahoma provides a guide and one-page roadmap of where technology in Oklahoma's state government is headed and how it is transforming to meet the growing citizen and business needs of our state.

Oklahoma is rapidly changing in economic, demographic and technological areas," noted CIO Bo Reese. "This plan will help Oklahoma continue to work together and collaborate on improving citizen services and our missions to provide those services with technology at the forefront."

Oklahoma's technology discussion is beginning to shift to IT investments and delivering business value. The strategic plan establishes a framework for improvement that includes identifying and sharing best practices; aligning technology governance and strategies to agency missions and business roadmaps; and improving network capability to rural areas, all while continuing our efforts to secure citizen data, our state's biggest asset.

"We have spent our efforts unifying IT over the past six years, finding efficiencies, getting rid of duplication and improving cybersecurity," said Reese. "Let's look to the future and see technology as a strategic investment."

The roadmap focuses on three channels: citizen, public sector employee and innovation.

- Citizen: This channel focuses on the experience citizens have with state government through technology from smart phones to citizen data.
- Public Sector Employee: This channel focuses on the needs of our public sector employees and technology use to improve delivery of services and business processes.
- Innovation: This channel outlines innovation technology initiatives for both citizens and private sector employees such as unmanned aerial vehicles, internet of things and blockchains.

View the Oklahoma IT Strategic Plan.

OMES

Oklahoma IT Strategic Plan

2017-2021