AGENDA
STATE GOVERNMENT COUNCIL
Executive Building - Lower Level Conference Room
521 S 14th Street
Lincoln, Nebraska
Thursday, August 11, 2016
1:30 p.m.

1:30 p.m.	1. Roll Call, Meeting Notice & Open Meetings Act Information 2. Public Comment 3. Approval of Minutes – June 9, 2016* *(Attachment 3)*	Chair
	4. Standards and Guidelines a. Proposed NITC 3-101 *(Attachment 4-a)* i. Ad Hoc Working Group b. Security Policy Framework *(Attachment 4-b)*	Chair Chris Hobbs
	5. CIO Update a. OCIO Public Information Officer, Holly West b. Roadmap c. Consolidation	Ed Toner
	6. Agency Reports and Other Business	Members
2:30 p.m.	7. Adjourn	Chair

* Denotes Action Item

The Council will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on June 23, 2016. The agenda was posted to the NITC website on August 9, 2016.

Nebraska Open Meetings Act

STATE GOVERNMENT COUNCIL
Executive Building - Lower Level Conference Room
521 S 14th Street Lincoln, Nebraska
Thursday, June 9, 2016, 1:30 p.m.
MINUTES

MEMBERS PRESENT:
Ed Toner, Chief Information Officer, Chair
Colleen Byelick, Secretary of State
Dennis Burling, Department of Environmental Quality
Keith Dey, Department of Motor Vehicles
Karen Hall, Alt. for Byron Diamond, Administrative Services
Bill Wehling, Department of Roads
Brent Gaswick, Department of Education
Kim Menke, Department of Natural Resources
Mike Fabry, Department of Banking
Glenn Morton, Workers' Compensation Court
Jim Ohmberger, OCIO-Enterprise Computing Services
Jennifer Rasmussen, State Court Administrator's Office
Jayne Scofield, OCIO-Network Services
Terri Slone, Department of Labor
Ron TeBrink, Department of Correctional Services
Rod Wagner, Library Commission

MEMBERS ABSENT: Mike Calvert, Legislative Fiscal Office; Dorest Harvey, Private Sector; Pam Kunzman, Nebraska State Patrol; Chris Hill, Department of Health and Human Services Gerry Oligmueller, Budget; and Mike Overton, Crime Commission

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

The Chair, Ed Toner, called the meeting to order at 1:30 p.m. There were 16 voting members present at the time of roll call. A quorum existed to conduct official business. Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on April 22, 2016. The agenda was posted to the NITC website on June 4, 2016. A copy of the Nebraska Open Meetings Act was located at the front of the room.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF FEBRUARY 11, 2016 MINUTES

Mr. Harvey moved to approve the February 11, 2016 minutes as presented. Mr. Dey seconded. Roll call vote: Toner-Yes, Byelick-Yes, Burling-Yes, Dey-Yes, Hall-Yes, Wehling-Yes, Gaswick-Yes, Menke-Yes, Fabry-Yes, Morton-Yes, Ohmberger-Yes, Rasmussen-Yes, Scofield-Yes, Slone-Yes, TeBrink-Yes, and Wagner-Yes. Results: Yes-16, No-0, Abstained-0. Motion carried.

OCIO ROADMAP UPDATE

Mr. Toner commented that it was just a year ago that he began his first day as the State's Chief Information Officer. Due to the collaboration and cooperation between the OCIO and state agencies, there has been a lot of progress made with the OCIO Roadmap. He has learned a lot and is still learning about state government and expressed appreciation to everyone helping him in accelerating his learning curve.

Consolidation Update. Phase 1 of the IT consolidation, which was networks, is done. The agencies impacted were DHHS, NDOR and NDCS. Appreciation was expressed for the cooperation in making this successful. Phase 2, which is server administration is underway. Phase 3 will be desktop consolidation and will not begin until sometime in Calendar year 17, after all cabinet agencies are on the enterprise domain. If there is an agency specific application, that agency IT staff would provide better support and that will stay with the agency.

Service Manager Update. This has been a cooperative and collaborative effort and rollout between the OCIO and the agencies. The OCIO will be meeting with agency representatives currently on Service Manager to address their issues and needs. Plans are underway to establish a "Service Manager User Group". The Change Management module is being tested internally and will be rolled out soon.

STANDARDS AND GUIDELINES

Amendments to NITC 1-201

> Purpose: By statute, "[o]n or before September 15 of each even-numbered year, all state agencies, boards, and commissions shall report to the Chief Information Officer, in a format determined by the commission, an information technology plan that includes an accounting of all technology assets, including planned acquisitions and upgrades." (Neb. Rev. Stat. § 86-524.01). This document contains the approved format for agency information technology plans.

The Office of the CIO is moving from a paper to an online form for agency IT plans. It will be released soon and will make it easier for agencies to update their plans.

Ms. Byelick moved to approve the proposed amendment to the agency IT plan. Ms. Kunzman seconded. After discussion, the council members made recommendations to the standard.

Ms. Byelick offered a friendly amendment, to the original motion to approve proposed amendments to NITC 1-201 and to include the council members approved changes below. Ms. Kunzman approved:

- **Section 1.5.1 Server Rooms: Add a question 11 indicated agency servers are housed with the OCIO.**
- **Section 3.1 Security: Include contact information for the State Security Officer**
- **Section 3.3 Geographic Systems:**
    - **Section 3.3 GIS: Delete last section regarding data backup. Per Nathan Watermeier, GIS Coordinator, this is being done via the OCIO GIS services.**
    - **Section 3.5 Mobile Apps: Delete this section**
    - **Section 3.6 Social Media: Delete this section.**

- **Section 4 Projects and Future Plans: For each section, agencies should indicate how the projects and future plans will align with their agency's goals on all**

Roll call vote: Slone-Yes, Burling-Yes, Hall-Yes, Byelick-Yes, Gaswick-Yes, Gittens-Yes, Harvey-Yes, Dey-Yes, Morton-Yes, Ohmberger-Yes, Fabry-Yes, Kunzman-Yes, Scofield-Yes, Sloup-Yes, Toner-Yes, and Wehling-Yes. Results: Yes-16, No-0, Abstained-0. Motion carried.

Proposed NITC 3-101 Cloud Computing Standard

Purpose: The Office of the Chief Information Officer ("OCIO") delivers IT solutions in a standards-based, technologically sound and secure environment. In alignment with the State's strategic direction for IT and to leverage the State's substantial investment in private cloud computing services, state agencies needing cloud computing services shall use the private cloud computing services provided by the OCIO ("State Cloud") unless an exception is granted as provided herein. If the State Cloud does not fully address an agency's business needs and the agency is considering a vendor provided cloud computing alternative, the agency shall submit a *Cloud Computing – Statement of Intent* (form attached hereto as "Attachment A") to the OCIO that outlines the requirements, costs and risks prior to proceeding with the initiative.

The agency's *Cloud Computing - Statement of Intent* shall be submitted to the OCIO during the planning/requirements gathering process of any project potentially utilizing a vendor provided cloud computing solution. Upon receiving the *Cloud Computing – Statement of Intent*, the OCIO will schedule a meeting with the agency to discuss the request. After reviewing the request, the OCIO may approve the exception; approve the exception with conditions; or deny the exception.

All purchase requests for cloud services shall be submitted using the IT procurement review process as outlined in NITC 1-204.

The standard has been posted for the 30-day comment period. Once the comment period is done, the standard will need to reviewed and approved by the NITC Technical Panel. If approved by the Technical Panel, the NITC will have the final review and approval. Council members were asked to review the standard and provide feedback and recommendations. Currently, the OCIO is a private cloud for state agencies but the OCIO is looking at a Hybrid Cloud solution that would also be secure and cost effective.

Recommendations from the council included:

- Page 2, include some generic definitions, state cloud, hybrid cloud, private cloud
- Public cloud section 4. The first sentence policy should be based on the data. Mr. Toner believed this sentence was supposed to be left out but will verify.
- Mr. Hobbs acknowledged that the OCIO needs to better and more frequently communicate to agencies IT staff about the NITC standards.

This will be an agenda item at the next Council meeting.

Report from the Security Architecture Workgroup on Security Standard, Chris Hobbs.

The Security Architecture Work Group has been working on fine tuning the NITC security Standards. The work group wants to include a section for enforcement of the Standard.

These recommendations will need to be voted on by the State Government Council, then to the Technical Panel who will make the recommendation to the NITC for final review and approval.

AGENCY REPORTS AND OTHER BUSINESS

Office of the CIO, Chris Hobbs. The Security Awareness Training is now available online to all employees via the Employee Development Center.

Department of Revenue, Len Sloup. Approximately 91.4% of Nebraska citizens filed their tax returns electronically this year. Nebraska is one of the top states for e-filing in the country. The agency moves over $5 million in revenue every month with the new application that is being used by citizens. The agency is working on a project with the Historical Society and the OCIO regarding historical tax credits.

Workers Compensation Court, Glen Morton. Mr. Morton announced that Aaron Anderson, is the agency's new ITcontact.

Nebraska State Patrol, Pam Kunzman. The agency has been working with the Department of Roads and will be bringing in other law enforcement agencies to be part of the TRACS e-citations application. An automatic vehicle location application is being developed with the Department of Roads as well. Kronos is being implemented for the time reporting and the agency is working on an interface between Kronos, E1 and Workday.

Department of Banking, Mike Fabry. The agency has been working with the OCIO on a project called Azure. Another new application being piloted is the banking examination for employees and peer-to-peer.

Department of Motor Vehicles, Keith Dey. They have been working with Purchasing to release an RFI released for the title and registration system that will have a self-contained architecture to provide a new platform that all DMV divisions can use. Vendors will be providing demonstrations during the last week in July. In preparation for these demonstrations, the agency has been reviewing data to look at conversion numbers, as well as doing data cleanliness.

ADJOURNMENT

Mr. Fabry moved to adjourn. Mr. Harvey seconded. All were in favor. Motion carried.

The meeting was adjourned at 2:48 p.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Jayne Scofield, Office of the CIO.

State of Nebraska
Nebraska Information Technology Commission
Standards and Guidelines

NITC 3-101 (Cloud Computing Standard)

A PROPOSED NEW STANDARD relating to cloud computing:

1. STANDARD

The Office of the Chief Information Officer ("OCIO") delivers IT solutions in a standards-based, technologically sound and secure environment. In alignment with the State's strategic direction for IT and to leverage the State's substantial investment in private cloud computing services, state agencies needing cloud computing services shall use the private cloud computing services provided by the OCIO ("State Cloud") unless an exception is granted as provided herein.

If the State Cloud does not fully address an agency's business needs and the agency is considering a vendor provided cloud computing alternative, the agency shall submit a *Cloud Computing – Statement of Intent* (form attached hereto as "Attachment A") to the OCIO that outlines the requirements, costs and risks prior to proceeding with the initiative.

The agency's *Cloud Computing - Statement of Intent* shall be submitted to the OCIO during the planning/requirements gathering process of any project potentially utilizing a vendor provided cloud computing solution. Upon receiving the *Cloud Computing – Statement of Intent*, the OCIO will schedule a meeting with the agency to discuss the request.

After reviewing the request, the OCIO may approve the exception; approve the exception with conditions; or deny the exception.

All purchase requests for cloud services shall be submitted using the IT procurement review process as outlined in NITC 1-204.

2. INQUIRIES AND SUBMISSION

Direct inquiries and the submission of the *Cloud Computing – Statement of Intent* to: OCIO.ITPurchase@nebraska.gov

3. DEFINITIONS

This document uses the National Institute of Standards and Technology (NIST) definition of cloud computing and corresponding service models:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models:

- ***Cloud Software as a Service (SaaS).*** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- ***Cloud Platform as a Service (PaaS).*** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- ***Cloud Infrastructure as a Service (IaaS).*** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

4. REQUIREMENTS AND CONSIDERATIONS

Requirements and considerations in this section are presented in summary form to illustrate key functional, technical and operational differences between each cloud offering and are meant to be representative as opposed to complete.

Legend: ✓**Preferred Solution**, △**Subject to Review**, ⊘**Not Acceptable**

Requirement Area	Key Considerations	State Cloud	Hybrid Offering	Public Cloud
	Infrastructure Suitability			
Security and Privacy	▪ Maintenance of Highly Restricted, Confidential, Managed Access Public and Public data (NITC 8-101) ▪ Resiliency to unauthorized access via unique encryption keys ▪ Data will never be co-mingled with that of other organizations.	✓	△	⊘
Technical Performance	▪ High CPU, Memory, Bandwidth or I/O Requirements ▪ Predictable workloads	✓	✓	△
Availability & Service Levels	▪ 24x365 availability, 99.95%+ uptime ▪ Fault tolerance, redundancy	✓	△	⊘
Customization	▪ Standards enforcement (OS, DBMS, Security, System Image) ▪ Tailored to Application / Agency technical requirements within standards	✓	△	⊘
Cost Savings Impact Areas	▪ Operational Cost of Ownership ▪ Ongoing TCO reduction, Cost avoidance	✓	✓	✓
Driver of Statewide Consolidation	▪ Reduction in systems, software and application counts, operational complexity ▪ Simplification of integration, workflows and labor requirements	✓	✓	✓
Migration Profile	▪ Ease of migration from current solution platform to cloud based offering ▪ Technical migration complexity profile	△	△	△
Integration (Process & Technical)	▪ Cross system workflow support and data exchange ▪ Mixture of sensitive and non-sensitive data ▪ Adherence to State integration standards	✓	△	⊘
	IT Application Profile Suitability			
Websites and Public Interaction (Informational)	▪ Presentation of State / Agency presence to public / businesses ▪ Distribution of non-sensitive data	✓	✓	✓
Transactional Websites	▪ Collection of non-sensitive transactional data ▪ Collection of low-risk fees/revenue or other information	✓	✓	△
Workgroup Enablement	▪ Storage of routine forms, data, knowledge management and other workgroup enablement data / functions	✓	✓	✓
Business Process Enablement	▪ Integrated processes within a single application or application suite ▪ Processing of transactional data non-critical to the State or public safety, revenue collection	✓	△	△
End User Computing	▪ Agency specific and non-critical applications ▪ Simple integration and reporting ▪ Routine Agency functions (non-sensitive data)	✓	✓	✓

Cross-Agency Systems	▪ Agency specific critical applications ▪ Complex integration and reporting ▪ Routine Agency functions (sensitive data)	✓	⊘	⊘
DR – Non Critical Systems / Data	▪ Data replication of non-sensitive systems and data ▪ Archive and reference data management	✓	✓	△
State ERP (E1)	▪ Operational Uptime and Performance ▪ Highly complex business rules and integration ▪ Maintenance of Sensitive Data	✓	⊘	⊘
Highly Integrated Operational Systems	▪ Complex integration and workflows, potentially spanning many systems and work groups ▪ High operational uptime and performance requirements ▪ Maintain personal or confidential data	✓	⊘	⊘
State Critical Systems	▪ Systems that directly influence the State's ability to perform Public Safety, Citizen Services, Revenue Collection and/or Critical Employee Services	✓	⊘	⊘

Attachment A - Cloud Computing Guidelines – Statement of Intent Submission Form

Date of Request:	**Requesting Agency**:	**Contact Person & Title:**

Phone Number:	**Address**:	**E-mail Address:**

Business rationale for selecting an alternative cloud computing solution *(Provide **specific business and / or technical reason(s)** why the agency/functional unit cannot use an existing State Cloud solution.)*:

Proposed cloud computing service model (*e.g., Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS*):

Deployment strategy (e.g., hybrid, private or public cloud):

Description of the maturity of the technologies involved (*Has successfully implemented in other government environment. If NE is the first customer for this technology, it is not mature)**:**

Estimated agency startup and ongoing maintenance costs of the proposed solution:

If a particular vendor is already under consideration, financial ability to perform the contract *(Can provide documentation showing other customers of same size using solution. Can provide documentation showing they have passed required federal audits)*:

Exit strategy/plan in the event that the agency is not satisfied with the cloud-based solution or the vendor is not able to provide the service:

Identification of the type of data that will be included in the proposed solution, including any sensitive data or personally identifiable information (Refer to http://nitc.ne.gov/standards/8-101.html for guidance on data types.):

Detail where and how state data will be stored, accessed, tested, maintained or backed-up:

Description of the agency's security policies and, if known, vendor security practices that are in place or will be implemented to safeguard the State of Nebraska's information assets from unauthorized disclosure, modification or destruction and to address the basic security elements of confidentiality, integrity and availability:

Identification of the proposed business continuity and disaster recovery plan that will be used to ensure the timely restoration, relocation or replacement of resources in the case of a disaster or other business interruption:

Explanation of incident response procedures in the event of a security breach, including the loss or theft of devices and media:

Approach to handling record retention, public record and e-discovery requirements in the proposed cloud computing solution:

Agency plans for providing help desk support for the proposed cloud-based solution:

High-level planning, design, development, implementation and maintenance timeline for the effort:

Requesting Agency Approval

Agency Director Approval Signature:
Date:

For OCIO Management Use Only

State Chief Information Officer (or his/her designee) Approval:
Approve ☐ Approve with Conditions ☐ Disapprove ☐
Conditions or Reason for Disapproval:

State Chief Information Officer (or his/her designee) Signature:
Date:

Please submit the completed form to: **OCIO.ITPurchase@nebraska.gov**

NITC 8-100: Information Security Policy

Category: Security Architecture

Applicability: Applied to all state government agencies, boards and commissions, excluding higher education institutions

History: Adopted on *month day,* 2016.

1. Purpose

The NITC has statutory responsibility to adopt minimum standards and guidelines for acceptable and cost-effective use of information technology, and to provide strategic direction for all State agencies and educational institutions for information technology.

The purpose of this Information Security Policy is to provide a uniform set of reasonable and appropriate security safeguards for protection of the confidentiality, integrity, and availability of State of Nebraska information collected, stored, and used to serve the citizens of the State of Nebraska. This Information Security Policy contains the safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

The components of this Information Security Policy encompass:

- 8-100 State of Nebraska Information Security Policy
- 8-200 General Provisions
- 8-300 Access Control
- 8-400 Network Security
- 8-500 System Security
- 8-600 Application Security
- 8-700 Auditing and Compliance
- 8-800 Vulnerability and Incident Management
- 8-900 Data Security.

2. Scope

This policy is applicable to State of Nebraska full-time and temporary employees, third-party contractors and consultants, volunteers and other agency workers (hereafter referred to as "Staff"), all State Agencies, Boards and Commissions (hereafter referred to as "Agency").

This Information Security Policy encompasses all systems, automated and manual, for which the State has administrative responsibility, including systems managed or hosted by third parties on behalf of an Agency.

Guidelines and standards, published by the NITC, which are associated with this policy, provide specific details for compliance with this ~~mandatory~~ Information Security Policy.

3. Roles and Responsibilities

State Agencies: Agencies that create, use or maintain information systems for the State of Nebraska must create and maintain an information security program that ensures the confidentiality, availability, and integrity of the State's information assets. And follow the standards and guidelines within this policy.

Office of Chief Information Officer

The Chief Information Officer is the executor of this Information Security Policy, which establishes and monitors the effectiveness of information security, standards and controls within the State of Nebraska. The Office of the CIO will modify this policy as directed by the NITC, or as needed to keep current with continually changing threats and technology.

State Information Security Officer

The State Information Security Officer, operating through the Office of the Chief Information Officer, performs as a security consultant to agencies and Agency Information Security Officers to assist the Agency in meeting the requirements of this policy. The State ISO may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Agency Information Security Officer

Agency Information Security Officers are obligated to provide requested updates of this policy to the State Information Security Officer. The Agency Information Security Officer has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the information security policies and standards. The Agency Information Security Officer is responsible for providing direction

and leadership to the agency through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes. The Agency Information Security Officer is responsible for investigating all alleged information security violations. In this role, the Agency Information Security Officer will follow agency procedures for referring the investigation to other investigatory entities, including law enforcement. The agency Information Security Officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives.

Nebraska Information Technology Commission (NITC)

The NITC is the owner of this policy with statutory responsibility to promote information security through adoption of policies, standards, and guidelines. The NITC develops strategies for implementing and evaluating the effectiveness of information security.

NITC Technical Panel

The NITC Technical Panel, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

NITC State Government Council

The NITC State Government Council, with advice from the Security Work Group, has responsibility for recommending security policies and guidelines and making available best practices to operational entities.

Third Party Vendors

Entities performing Information Technology services for the state of Nebraska must adhere to this policy standards and guidelines.

4. Operational and Functional Responsibilities

Operational and Functional Responsibilities will be covered in a subsequent Standard.

8. Security Architecture

- **8-100 State of Nebraska Information Security Policy**
  - **a. Purpose**
  - **b. Scope**
  - **c. Roles and Responsibilities**
  - **d. Operational and Functional Responsibilities**

- **8-200. General Provisions**
  - **8-201. Acceptable Use Policy**
  - **8-202. Media Protection and Sanitization**
  - **8-203. Personnel Security**
    - **New Hires**
    - **Terminations**
    - **Segregation of Duties**
  - **8-204. Procurement**
  - **8-205. Software Inventory**
  - **8-206. Hardware Inventory**
  - **8-207. Change Control Management**
  - **8-208. Identification Badges**
  - **8-209. Operational and Functional Responsibilities**
  - **8-210.**
  - **8-211.**

- **8-300. Access Control Security Standard**
  - **8-301. Remote Access Standard**
  - **8-302. Monitoring User Access**
  - **8-303. Minimum Password Configuration**
  - **8-304. Identification and Authorization**

- **8-400. Network Security Standard**
  - **8-401. Network Documentation**
  - **8-402. Data Transmission Security**

- **8-500. System Security Standard**
  - **8-501. System Documentation**
  - **8-502. Minimum User Account Configuration**
  - **8-503. Patch Management**
  - **8-504. Minimum Server Configuration**
  - **8-505. Minimum Workstation Configuration**
  - **8-506. Minimum Laptop Configuration**
  - **8-507. Minimum Mobile Device Configuration**

- **8-600. Application Security Standard**
  - **8-601. Application Documentation**
  - **8-602. Separation of Test and Production Environments**
  - **8-603. Application Development**
  - **8-604. Cloud Security**

8-700. Auditing and Compliance Security Standard

- **8-701. Awareness and Training**
- **8-702. Security Reviews**
- **8-702. PCI Compliance**
- **8-703. HIPAA Compliance**
- **8-704. CJIS Compliance**
- **8-705. IRS Compliance**
- **8-706. SSA Compliance**
- **8-707. APA Compliance**

8-800. Vulnerability and Incident Management Security Standard

- **8-801. Incident Response**
- **8-802. Penetration Testing**
- **8-803. Vulnerability Scanning**
- **8-804. Malicious Software Protection**

8-900. Data Security Standard

- **8-901. State of Nebraska Information Sharing**
- **8-902. Data Inventory**
- **8-903. Data Classification**