TECHNICAL PANEL
Virtual Meeting
Tuesday, April 13, 2021
9:00 a.m. CT

Join Zoom Meeting
https://zoom.us/j/96876159030
(Additional Zoom meeting options provided on page 4.)

AGENDA

I. ROLL CALL; MEETING NOTICE; OPEN MEETINGS ACT INFORMATION

II. APPROVAL OF FEBRUARY 9, 2021 MEETING MINUTES* *(Attachment II)*

III. PUBLIC HEARING - TECHNOLOGY ACCESS CLAUSE*

Notes for the public hearing on the technology access clause:

- **Background.** Pursuant to Neb. Rev. Stat. § 73-205, representatives from the Commission for the Blind and Visually Impaired, the Nebraska Information Technology Commission, and the Chief Information Officer, in consultation with other state agencies, developed a revised technology access clause to be included in all contracts entered into by state agencies. The revised clause would replace the current technology access clause adopted in December 2000 (https://nitc.nebraska.gov/standards/2-201.pdf).
- **Public Comment at the Hearing.** The purpose of the hearing is to accept public comments on the revised technology access clause. Public comments during the virtual hearing will be made using Zoom video conferencing. To assist in making the Zoom connection, those wishing to comment are asked to contact the Technical Panel at ocio.nitc@nebraska.gov or 402-471-7984 at least 24 hours prior to the hearing. Each speaker will be limited to 5 minutes. The hearing is scheduled for one hour but may end earlier if commenting has concluded.
- **Written Comments.** Written comments may be submitted by email to ocio.nitc@nebraska.gov at least 24 hours prior to the hearing.
- **Revised Technology Access Clause.** The revised clause follows:

Technology Access Assurances:

1.) Commitment: The State of Nebraska is committed to ensuring that all information and communication technology (ICT), developed, leased, or owned by the State of Nebraska, affords equivalent access to employees, program participants and members of the public with disabilities, as it affords to employees, program participants and members of the public who are not persons with disabilities.

2.) Understanding and warrantee: By entering into this Contract, Contractor understands and agrees that if the Contractor is providing a product or service that contains ICT, as defined in (subsection XX), and such ICT is intended to be directly interacted with by the user or is public-facing, such ICT must provide equivalent access, or be modified during implementation to afford equivalent access, to employees, program participants, and members of the public who have and who do not have disabilities. The Contractor may comply with section by complying with Section 508 of the Rehabilitation Act of 1973, as amended, and its implementing standards adopted and promulgated by the U.S. Access Board.

3.) Scope of ICT: ICT means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Contractor hereby agrees ICT includes computers and peripheral equipment, information kiosks and transaction machines, telecommunications equipment, customer premises equipment, multifunction office machines, software; applications, web sites, videos, and electronic documents. For the purposes of these assurances, ICT does not include ICT that is used exclusively by a contractor.

IV. REGULAR BUSINESS

a. Projects.
    i. Enterprise project status dashboard. Andy Weekly. *(Attachment IV-a-i)*
    ii. Recommend designating the Financial Systems Modernization Project as an enterprise project.*
b. Technical standards and guidelines.

i. Proposal 18. Change provisions of the Information Security Policy.* [Motion to recommend approval.] *(Attachment IV-b-i)*
ii. Proposal 19. Amend the minimum server configuration standard.* [Motion to post for 30-day comment period.] *(Attachment IV-b-ii)*

c. Work group updates; other business.

V. ADJOURN

* Indicates an action item.

This is a virtual meeting of the Technical Panel conducted pursuant to Neb. Exec. Order No. 21-02 (http://govdocs.nebraska.gov/docs/pilot/pubs/eofiles/21-02.pdf). No quorum of the body will be physically present together, and there will be no public in-person attendance.

The Technical Panel will attempt to adhere to the sequence of the published agenda but reserves the right to adjust the order and timing of items and may elect to take action on any of the items listed. If you need interpreter services or other reasonable accommodations, please contact the Technical Panel at 402-471-3560 at least five days prior to the meeting to coordinate arrangements.

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on April 1, 2021. The agenda was posted to the NITC website on April 1, 2021.

Nebraska Open Meetings Act | Technical Panel Meeting Documents

ZOOM MEETING OPTIONS

Topic: NITC Technical Panel Meeting
Time: Apr 13, 2021 09:00 AM Central Time (US and Canada)

Join Zoom Meeting
https://zoom.us/j/96876159030

Meeting ID: 968 7615 9030
One tap mobile
+13462487799,,96876159030# US (Houston)

Dial by your location
+1 346 248 7799 US (Houston)
+1 312 626 6799 US (Chicago)
Meeting ID: 968 7615 9030
Find your local number: https://zoom.us/u/acobG9kkWs

Join by SIP
96876159030@zoomcrc.com

Join by H.323
162.255.37.11 (US West)
162.255.36.11 (US East)
Meeting ID: 968 7615 9030

Attachment II

TECHNICAL PANEL
Tuesday, February 9, 2021, 9:00 a.m. CT 9:00 a.m.
Virtual Meeting
MINUTES

MEMBERS PRESENT:
Kirk Langer, Chair, Lincoln Public Schools
Ed Toner, Chief Information Officer, State of Nebraska
Ling Ling Sun, Nebraska Educational Telecommunications
Jeremy Sydik, University of Nebraska

MEMBERS ABSENT: Bret Blackman, University of Nebraska, ITS

ROLL CALL; MEETING NOTICE; OPEN MEETINGS ACT INFORMATION

Mr. Langer called the meeting to order at 9:04 a.m. The meeting was being conducted using videoconferencing, no quorum of the body was physically present together. Instructions for public access were included with the published agenda. Roll call was taken. A quorum was present. Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on January 22, 2021. The agenda was posted to the NITC website on February 5, 2021. A link to of the Nebraska Open Meetings Act was provided in the meeting materials.

PUBLIC COMMENT

There was no public comment.

APPROVAL OF OCTOBER 30, 2020 MEETING MINUTES

Ms. Sun moved to approve the October 30, 2020 meeting minutes as presented. Mr. Sydik seconded. Roll call vote: Toner-Yes, Sydik-Yes, Langer-Yes, and Sun-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

ELECTION OF TECHNICAL PANEL CHAIRPERSON FOR 2021

Mr. Toner nominated Kirk Langer to serve as the 2021 Chair of the NITC Technical Panel. There were no more nominations. Mr. Langer accepted the nomination.

Mr. Toner moved to elect Kirk Langer to serve as the 2021 Technical Panel Chair. Ms. Sun seconded. Roll call vote: Sun-Yes, Langer-Yes, Sydik-Yes, and Toner-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

PROJECTS
Andy Weekly, OCIO Project Manager

Mr. Weekly provided an update on the status of the enterprise projects.

Enterprise project closure. Dept. of Health and Human Services, New Medicaid Management Information System (MMIS) project

Mr. Weekly stated that the project is in full implementation and operational.

Mr. Toner moved to recommend closure of the MMIS project. Ms. Sun seconded. Roll call vote: Sydik-Yes, Langer-Yes, Sun-Yes, and Toner-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

TECHNICAL STANDARDS AND GUIDELINES

Request for Waiver 20-03. Department of Transportation

The Department of Transportation's Aeronautics website was designed through Wix. Wix does not allow for external SSL certifications and they will not give an SSL certification to an external domain. This was discovered after the website was implemented. The agency has worked with the OCIO and will migrate to a .gov website by the end of their subscription period in October.

Mr. Toner moved to approve Request for Waiver 20-03 with an expiration date of November 1, 2021. Ms. Sun seconded. Roll call vote: Langer-Yes, Sydik-Yes, Toner-Yes, and Sun-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

Proposal 18. Change provisions of the Information Security Policy

Patrick Wright, State Security Information Officer, introduced the proposal. Members discussed the proposal.

Ms. Sun moved to post Proposal 18 for the 30-day comment period. Mr. Sydik seconded. Roll call vote: Toner-Yes, Sydik-Yes, Langer-Yes, and Sun-Yes. Results: Yes-4, No-0, Abstained-0. Motion carried.

WORK GROUP UPDATES; OTHER BUSINESS

Tim Cao, IT Administrator OCIO Operations, reported on the AS400 consolidation initiative. The last seven remaining counties—Adams, Cedar, Clay, Gage, Kearney, Richardson and Scotts Bluff—have agreed to participate in the server consolidation initiative. Once this is completed, the OCIO will be hosting 87 county AS400 servers.

ADJOURNMENT

Mr. Toner moved to adjourn. Ms. Sun seconded. All were in favor. Motion carried.

The meeting was adjourned at 10:00 a.m.

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

Attachment IV-a-i

Projects Status Dashboard

April 2021

Enterprise Projects - Current

Agency/Entity	Project	NITC Designated
Nebraska Council of Regions	Nebraska Regional Interoperability Network	03/15/2010
Office of the CIO	Centrex Replacement	07/12/2018
Department of Health and Human Services	iServe Nebraska	11/12/2020

Note: Status is self-reported by the agency

Project Storyboard: Centrex Conversion

Project Manager	Kortus, Julie	Status Report Date	4/1/21
Project Type	Major Project	Status	Approved
Stage	Build	Progress	Started
Total Estimated Cost	$2,800,000.00	Estimate to Complete	
Actual Cost To Date			

Project Dates

	Start	Finish
Plan	10/10/17	12/31/22
Baseline	10/10/17	12/31/22
Days Late	0	0

Status Report Indicators

Overall	
Schedule	
Scope	
Cost and Effort	

Project Description

To secure the most cost efficient Hosted Voice Over Internet Protocol Telephony (VOIP) Services. This solution will replace the State's Centrex service throughout the State of Nebraska. The purpose of the project is to provide phone service that includes the most up-to-date VOIP features and functionality as a hosted service with equipment ownership, maintenance and service remaining with the Contractor.

Key Accomplishments

Status Report Update

As of 3/31/2021:
6416 lines have been converted to Allo.
400 lines belong to agencies that will not be converting
591 lines were moved off of the Centrex contract and onto a new B1 contract.

10,000 lines were in the RFP to be taken off of the Centrex contract from Windstream and CenturyLink territory.

Project is 74.1% complete.

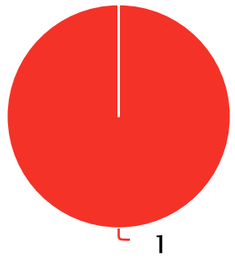
The OCIO Voice Team continues to work with the remaining Windstream lines. Allo is working with agencies in the CenturyLink territory.

In parallel with this project, over 800 softphones have been deployed using the same resources assigned to this project.

Upcoming Activities

Issues by Priority

Risks by Priority



Current Risks

More Risks...

Risk	Probability	Impact	Priority	Status	Target Resolution	Owner
Bandwidth at Sites				Work in Progress	6/30/20	Kortus, Julie

Project Storyboard: iServe Nebraska

Project Manager	Agarwal, Ankush	Status Report Date	3/24/21
Project Type	Major Project	Status	Approved
Stage	Design	Progress	Started
Total Estimated Cost	$11,200,000.00	Estimate to Complete	16.96%
Actual Cost To Date	$1,900,000.00		

Project Dates

	Start	Finish
Plan	4/6/20	10/1/21
Baseline	4/6/20	9/30/21
Days Late	1	1

Status Report Indicators

Overall	
Schedule	
Scope	
Cost and Effort	

Project Description

IHHS - Clarity Plan for IS&T Contractors Timesheets JC 266171 WO 266110 April 2020 thru Sept 30 2021.
7/28/2020 Project Name & Timesheets Change to iServe JC/WO number remained same.
10/21/20 PM name from Annette Pilcher to Ankush Agarwal

Key Accomplishments

First Work Orders released to Vendor Pool for bid with responses due this week.
Federal funding request for Implementation budget submitted.

Status Report Update

Key Activities on Track. First Work Orders for Portal released to Vendor Pool for bid. Beginning stand-up of foundational infrastructure and Cloud Environments. Development of RFQ for Integrated Eligibility and Enrollment system continues.

Upcoming Activities

Award first work orders and kick-off associated work streams.
Release next work order(s)
Continue foundational infrastructure stand-up

Issues by Priority

Risks by Priority

Current Issues

No matching records were found

Project Storyboard: Nebraska Regional Interoperability Network (NRIN)

Project Manager	Krogman, Sue	Status Report Date	4/7/21
Project Type	Major Project	Status	Approved
Stage	Build	Progress	Started
Total Estimated Cost	$12,500,000.00	Estimate to Complete	83.24%
Actual Cost To Date	$10,405,204.00		

Project Dates

	Start	Finish
Plan	10/1/10	8/31/21
Baseline	10/1/10	8/31/21
Days Late	0	0

Status Report Indicators

Overall	
Schedule	
Scope	
Cost and Effort	

Project Description

The Nebraska Regional Interoperability Network (NRIN) is a project that will connect a majority of the Public Safety Access Points (PSAP) across the State by means of a point to point microwave system. The network will be a true, secure means of transferring data, video and voice. Speed and stability are major expectations; therefore there is a required redundant technology base of no less than 100 mbps with 99.999% availability for each site. It is hoped that the network will be used as the main transfer mechanism for currently in-place items, thus imposing a cost-saving to local government. All equipment purchased for this project is compatible with the networking equipment of the OCIO.

Key Accomplishments

Investment Justifications have been created and submitted for grant dollars to continue the build-out.

Status Report Update

UPDATE FOR APRIL 2021 – There have been no installations done since the last NITC report due to the weather. Pre-work to ready equipment and materials are being done in the warehouse as well as requests for path designs and structural analysis. Having these ready to go will allow the installations to go smoother and faster.

UPDATE FOR JANUARY 2021 – Work in the NE Region has continued to be steady until this latest snow-storm. During this time the contractor is continuing to do prep work in their warehouse. Investment Justifications have been created and submitted for grant dollars to continue the build-out.

Upcoming Activities

Issues by Priority | Risks by Priority

Current Issues

No matching records were found

Attachment IV-b-i

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 18

A PROPOSAL relating to the Information Security Policy; to amend sections 8-103, 8-209, 8-210, and 8-211; to adopt a new section relating to public accounts; to repeal the original sections; and to outright repeal section 8-212.

Section 1. Section 8-103 is amended to read:

8-103. Roles and responsibilities.

(1) State Agencies. Agencies that create, use, or maintain information systems for the state must establish and manage an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the state's information assets. Agencies may work with the Office of the Chief Information Officer for assistance with implementing an information security program.

(2) Office of the Chief Information Officer. The Office of the Chief Information Officer is responsible for recommending policies and guidelines for acceptable and cost-effective use of information technology in noneducation state government.

(3) State Information Security Officer. The state information security officer serves as a security consultant to agencies and agency information security officers to assist the agencies in meeting the requirements of this policy and other policies. The state information security officer may also perform assessments of agency security for risk and compliance with this policy and ~~the NIST Cybersecurity Framework~~other security related policies and frameworks as applicable.

(4) Agency Information Security Officer. An agency information security officer may be designated at the discretion of the agency. The agency information security officer has the

responsibility for ensuring implementation, enhancement, monitoring, and enforcement of information security policies and standards for their agency. The agency information security officer may collaborate with the Office of the CIO on information security initiatives within the agency.

(5) Nebraska Information Technology Commission. The Nebraska Information Technology Commission is the owner of this policy with statutory responsibility to adopt minimum technical standards, guidelines, and architectures.

(6) Technical Panel. The Technical Panel is responsible for recommending technical standards and guidelines to be considered for adoption by the Nebraska Information Technology Commission.

(7) State Government Council. The State Government Council is an advisory group chartered by the Nebraska Information Technology Commission to provide recommendations relating to state government agencies.

(8) Security Architecture Workgroup. The Security Architecture Workgroup is chartered by the State Government Council to make recommendations to the State Government Council and Technical Panel on matters relating to security within state government; provide information to state agencies, policy makers, and citizens about real or potential security threats or vulnerabilities that could impact state business; document and communicate existing problems, potential points of vulnerability, and related risks; and determine security requirements of state agencies stemming from state and federal laws, regulations, and other applicable standards.

Sec. 2. Section 8-209 is amended to read:

8-209. ~~State and agency~~Agency security planning and reporting.

~~The following standard and recurring reports are required to be produced by the state information security officer and each agency information security officer; these reports will reflect the current and planned state of information security at the agency~~Pursuant to the terms

of certain federal data exchange agreements, state agencies may be required to maintain the following documentation:

(1) Information security strategic plan (section 8-210);

(2) System security plan (section 8-211); and

(3) ~~Plan of action and milestones report (section 8-212)~~Other information security documentation not covered by this section.

For agencies not subject to federal data exchange agreements, these planning documents are considered guidelines and recommended as best practice.

Sec. 3. Section 8-210 is amended to read:

8-210. Information security strategic plan.

Proper risk-based planning is critical to ensure the most appropriate projects are prioritized and funded by the state and its agencies. Information security planning is no exception. Planning for information protection should be given the same level of executive scrutiny at the state as planning for information technology changes. This plan ~~must~~ should be updated and published on ~~an annual~~a biennial basis, and should include a ~~5~~two-year projection of key security business drivers~~,~~ and planned security infrastructure implementation~~, and forecasted costs~~. ~~It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to state information assets.~~ This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall planning process.

Contents of the information security strategic plan:

(1) Summary of the information security, mission, scope, and guiding principles;

(2) Analysis of the current and planned technology and infrastructure design, and the corresponding changes required for information security to stay aligned with these plans;

(3) Summary of the overall information risks assessments and current risk levels. ~~Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks~~;

(4) Assessment of the current information security posture related to the future targeted posture, identified gaps, and high-level timeline necessary to close or mitigate those gaps;

(5) Summary of the policies, standards, and procedures for information security, and projected changes necessary to stay current and relevant;

(6) Summary of the information security education and awareness program, progress, and timeline of events;

(7) Summary of disaster recovery and business continuity activity and plans if the agency is required to maintain these documents by other requirement or policy;

(8) Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect information security; and

(9) Proposed ~~five~~two-year timeline of events and key deliverables or milestones.~~; and~~

~~(10) Line item cost projections for all information security activity that is itemized by:~~

~~(a) Steady state investments: The costs for current care and maintenance of the information security program;~~

~~(b) Risk management and mitigation: The line item expenses necessary to mitigate or resolve security risks for the agency in a prioritized order;~~

~~(c) Future technology: The line item forecasted expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats; and~~

~~(d) Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.~~

Sec. 4. Section 8-211 is amended to read:

8-211. System security plan.

The ~~state and agency~~ system security plan (SSP) provides an overview of the security requirements of the information system including all in-house or commercially developed and maintained systems and installations and to all external business partner systems and installations operated by, or on behalf of the state. The SSP describes the controls in place or

planned for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system. The SSP ~~will address all control areas identified in the NIST SP 800-53 control framework, and~~ will describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

~~The state information security officer will work with each agency information security officer to maintain an SSP incorporating each identified system managing information or used to process agency business.~~

The agency information security officer ~~and the state information security officer are required to~~ should develop or update the SSP in response to each of the following events: new system; ~~major~~ significant system modification; increase in security risks/exposure; increase of overall system security level; serious security violation(s); or every three years (minimum) for an operational system.

Contents of the system security plan:

(1) System name and title, description and scope of system including each all in-house or commercially developed system and installations included in the SSP;

(2) Responsible organization: Name and contact information for business area responsible for the systems defined in the SSP. Decision authority for business functionality and business risks;

(3) Key contacts: Name and contact information for personnel who can address system characteristics and operation. IT maintenance personnel for the system, applications, and infrastructure;

(4) System operation status and description of the business process, including a description of the function and purpose of the systems included in the SSP;

(5) System information and inventory, including a description or diagram of system inputs, processing, and outputs. ~~Describe information flow and how information is handled.~~ Include the

information classification for all information processed, accessed, or exposed. Include a system network and workflow diagram;

(6) A detailed diagram showing the flow of ~~sensitive~~ information~~, including CONFIDENTIAL and RESTRICED information~~. Describe details where this data is stored, accessed, or processed and include details of the security mechanisms applicable to this type of data;

~~(7) Detailed information security descriptions, procedures, protocols, and implemented controls for all NIST SP 800-53 control areas within the scope of the system. Identify compensating controls or compliance gaps within this section of the SSP;~~

~~(8) System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners;~~

~~(9)~~(7) Applicable laws, regulations, or compliance requirements: List any laws, regulations, or specific standards, guidelines that specify requirements for the confidentiality, integrity, or availability of information in the system;

~~(10)~~(8) Review of security controls and assessment results that have been conducted within the past three years; and

~~(11)~~(9) Information security risk assessment which includes identification of potential threat/vulnerabilities in the information system, analysis of planned or actual security controls, and potential impacts on operations, assets, or individuals.

Sec. 5. The following new section is adopted:

8-302.1 Public accounts; passwords.

This section sets forth the format, minimum requirements, and review procedures for public accounts accessing state resources. This section applies to all public accounts created for use within the State of Nebraska domain namespaces. Public accounts are accounts on state managed systems that are to be used by the general public and are not to be used by state employees or contractors to conduct state business.

(1) Information Access. A public account may only be used by the user to access their own information.

(2) Passwords. The following are the minimum requirements for public account passwords:

(a) Must contain a minimum of 12 characters;

(b) Must contain at least three of the following four complexity requirements: at least one uppercase letter; at least one lowercase letter; at least one numeric value; or, at least one special character; and

(c) Accounts must be locked temporarily after five failed password attempts.

(3) Review Process. Accounts with no successful login activity for a period of 24 months will be disabled. Accounts with no successful login activity for 26 months will be deleted.

(4) Misuse or Abuse. Any misuse or abuse of a public accounts will cause the account in question to be terminated.

Sec. 6. Original sections 8-103, 8-209, 8-210, and 8-211 are repealed.

Sec. 7. The following section is outright repealed: Section 8-212.

Sec. 8. This proposal takes effect when approved by the commission.

Attachment IV-b-ii

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 19

A PROPOSAL relating to the Information Security Policy; to amend sections 8-503; and to repeal the original section.

Section 1. Section 8-503 is amended to read:

8-503. Minimum server configuration.

The state recognizes the National Institute of Standards and Technology (NIST) along with Center for Internet Security (CIS) Controls and Benchmarks as ~~a~~ sources for recommended security requirements that provide minimum baselines of security for servers.

NIST and CIS provide~~s~~ instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST and CIS Control documents when installing or configuring servers. The documents are not all inclusive, but rather meant as a means of prompting and guiding administrators through the installation process.

Agencies must comply with the following NIST standards, guidelines, and checklists: NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations; NIST SP 800-70, National Checklist Program for IT Products; and NIST SP 800-44, Guidelines on Securing Public Web Servers. Agencies should also strive to implement the highest tier possible for the CIS Controls and Benchmarks.

Server Hardening. All State of Nebraska servers ~~that store, process, or have access to CONFIDENTIAL or RESTRICTED data~~ are required to be hardened according to these standards. In addition, these servers must have a published configuration management plan as

defined below and approved by the ~~state information security officer~~Office of the CIO. The following are server hardening standards:

(1) Servers may not be connected to the state network until approved by the Office of the CIO. This approval will not be granted for ~~sensitive~~ servers until these hardening standards have been met or risk levels have been accepted by agency management;

(2) The operating system must be installed by ~~IT~~ authorized IT personnel only, and all vendor supplied patches must be applied. All software and hardware components ~~should~~ must be currently supported by the vendor. All unsupported hardware and software components must be identified and have a management plan for replacement that is approved by the ~~state information security officer~~Office of the CIO;

(3) All unnecessary software, system services, system and admin accounts, and drivers must be removed or disabled unless doing so would have a negative impact on the server;

(4) Logging of auditable events, as defined in NIST SP 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access and retained for a minimum of one year or be retained in accordance with federal and state guidance;

(5) Security parameters and file protection settings must be established, reviewed, and approved by the ~~state information security officer~~Office of the CIO;

(6) All system software must have security updates and patches applied when made available from the vendor. Priority setting of vulnerabilities will be based on impact to the agency and as referenced in the National Vulnerability Database (https://nvd.nist.gov);

(7) ~~Hardened s~~Servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines;

(8) ~~Hardened s~~Servers will be monitored with active intrusion detection, intrusion protection, ~~or~~ and end-point security monitoring that has been approved by the state information security

officer. This monitoring must have the capability to alert IT administrative personnel within 1 hour;

(9) Servers must be loaded from standardized processes and software. These processes and software shall be appropriately configured and protected, with integrity controls to ensure only authorized and documented changes are possible;

(10) All significant changes to ~~hardened~~ servers must go through a formal change management and testing process to ensure the integrity and operability of all security and configuration settings. Significant changes must have a documented security impact assessment included with the change; ~~and~~

(11) Remote management of ~~hardened~~ servers must be performed over secured channels only. Protocols ~~such as telnet, VNC, RDP, or others~~ that do not actively support approved encryption, such as telnet, VNC, and RDP, should only be used if they are performed over a secondary encryption channel, such as ~~SSL or IPSEC~~TLS; and

~~(11)~~(12) Agencies must implement prevention techniques to protect against unauthorized data mining of information from public facing systems (e.g. Captcha).

Sec. 2. Original sections 8-503 is repealed.

Sec. 3. This proposal takes effect when approved by the commission.