AGENDA
NEBRASKA INFORMATION TECHNOLOGY COMMISSION
Northeast Community College
Lifelong Learning Center, Suites C & D
801 East Benjamin Avenue
Norfolk, Nebraska
Wednesday, July 12, 2017
10:00 a.m.

10:00 a.m.	1. Call to Order; Roll Call; Meeting Notice; and Open Meetings Act Information 2. Public Comment 3. **Approval of Minutes - March 9, 2017*** *(Attachment 3)*	Chair
10:15 a.m.	4. Reports from the Advisory Councils and Technical Panel	
	a. Community Council Report *(Attachment 4-a)* i. **Approve membership*** ii. Nebraska Broadband Today! Conference, October 26, 2017 iii. Nebraska Library Commission's Makerspace Grant *(Hyperlink)* iv. Nebraska and the Digital Divide Index *(Hyperlink)*	Anne Byers
	b. eHealth Council Report *(Attachment 4-b)* i. ONC grant update ii. NeHII Annual Meeting, August 3, 2017 iii. Action items update	
	c. Education Council Report *(Attachment 4-c)* i. **Approve membership*** ii. Action items update	Tom Rolfes
	d. GIS Council Report *(Attachment 4-d)* i. **Approve Nebraska Statewide Imagery Program-Business Plan*** ii. Update on Public Service Commission consolidation efforts iii. Update on Department of Transportation GIS consolidation/integration efforts iv. Update on ESRI GIS license consolidation efforts	John Watermolen
	e. Technical Panel Report i. Technical Standards and Guidelines 1. **Approve Proposal 17-02 Definitions*** *(Attachment 4-e-i-1)* 2. **Approve Proposal 17-01 Information Security Policy*** *(Attachment 4-e-i-2)*	Walter Weir

		ii. Enterprise Projects; Project Status Dashboard *(Attachment 4-e-ii)*	
		f. State Government Council Report *(Attachment 4-f)*	Ed Toner
		i. Update on CIO Roadmap	
11:45a.m.	5.	**Approve strategic initiatives to be included in the Statewide Technology Plan for 2017-2018*** *(Attachment 5)*	Chair
12:00 p.m.	6.	Adjourn	Chair

*** Indicates an action item.**

The Commission 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.

Meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on June 14, 2017. The agenda was posted to the NITC website on June 30, 2017.

Nebraska Open Meetings Act

Future Meeting Dates:

- November 9, 2017
- March 8, 2018
- July 12, 2018

Attachment 3

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

Nebraska Governor's Residence - Lower Level
1425 H Street, Lincoln, Nebraska
Thursday, March 9, 2017, 10:00 a.m.
MINUTES

MEMBERS PRESENT:

Senator Bruce Bostelman, Nebraska Legislature
Shane Greckel, Greckel Farms, LLC
Dr. Terry Haack, Bennington Public Schools
Dorest Harvey, US Strategic Command/J84
Randy Meininger, Mayor, City of Scottsbluff
Dan Shundoff, Intellicom
Dan Spray, Precision Technologies, Inc.
Walter Weir, University of Nebraska

MEMBERS ABSENT:

Ed Toner, Chief Information Officer, Chair
Gary Warren, Hamilton Telecommunications

CALL TO ORDER; ROLL CALL; MEETING NOTICE; AND OPEN MEETINGS ACT INFORMATION

In the absence of the Chair, Walter Weir presided over the meeting. The meeting was called to order at 10:05 a.m. Roll call was taken and found seven voting members present to achieve a quorum. The meeting notice was posted to the NITC website and the Nebraska Public Meeting Calendar on February 22, 2017. The agenda was posted to the NITC website on March 3, 2017. A copy of the Nebraska Open Meetings Act was located on the table located in the back of the room.

APPROVAL OF MINUTES - NOVEMBER 10, 2016*

Commissioner Shundoff asked that the minutes be corrected to reflect that he was not present at the November meeting.

Commissioner Shundoff moved to approve the November 10, 2016 meeting minutes as corrected. Commissioner Haack seconded. Roll call vote: Greckel-Yes, Haack-Yes, Harvey-Yes, Meininger-Yes, Shundoff-Yes, Spray-Yes, and Weir-Yes. Results: Yes-7, No-0, Abstained-0. Motion carried.

PUBLIC COMMENT

There was no public comment.

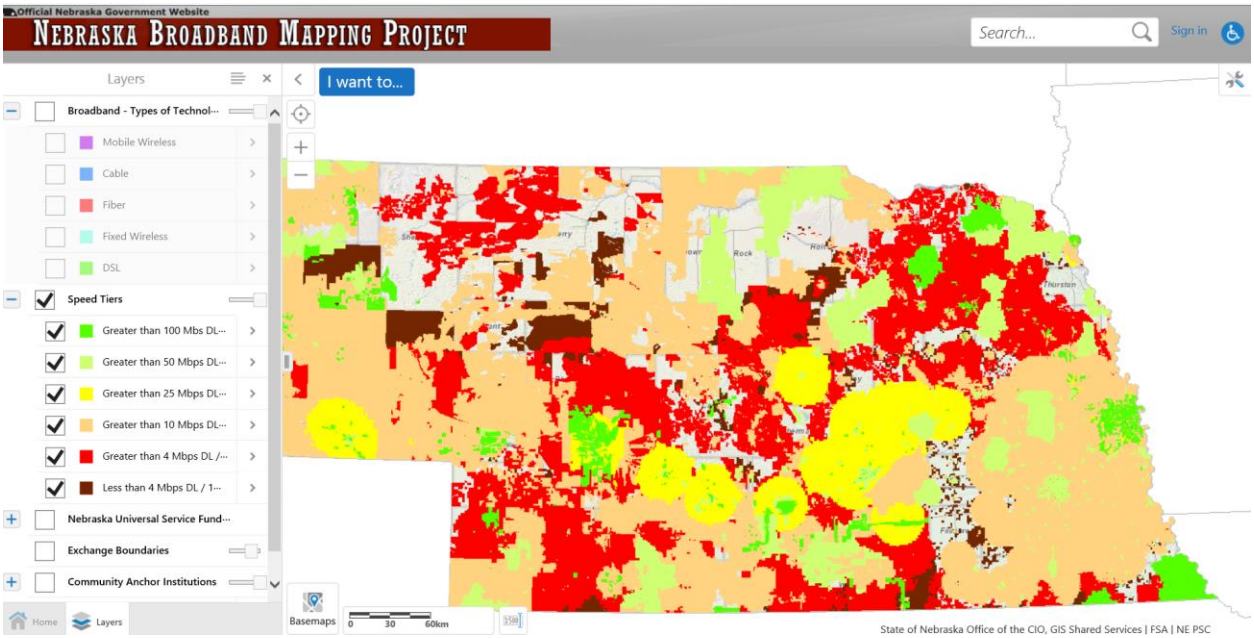
REPORTS FROM THE ADVISORY COUNCILS AND TECHNICAL PANEL

COMMUNITY COUNCIL REPORT

Anne Byers, Community IT Coordinator

The Community Council will meet on May 12 from 9:30 a.m. to noon in Lincoln.

Broadband Map. The Nebraska Broadband Map (broadbandmap.nebraska.gov) has been updated. The map below shows availability by speed tier.



Newsletter. The winter issue of *Nebraska Broadband* featured articles on Gallup's high school computer coding internship program, the need for students to have access to broadband to complete homework, Norfolk Public Library's hotspot lending program, and Lincoln Public Schools' hotspot lending program. The newsletter is one way to share lessons learned from exemplary programs across the state and to share updates on broadband-related issues.

Broadband Nebraska Today! Planning has begun for the Broadband Nebraska Today! Conference in October. The conference is sponsored by the Nebraska Telecommunications Association in partnership with the Nebraska Broadband Initiative.

EHEALTH COUNCIL REPORT

Anne Byers, eHealth IT Coordinator

Updates on Initiatives

The eHealth Council will meet on April 5 from 1:30 to 4:00 at the 1526 Building in Lincoln.

Nebraska Advance Interoperable Health IT Services to Support HIE Grant. The NITC received a 2-year $2.7 million Nebraska Advance Interoperable Health IT Services to Support Health Information Exchange grant from the Office of the National Coordinator in July 2015. Partners include NeHII and UNMC. Focus areas include: Critical Access Hospitals, long-term care facilities, and public health/researchers. Implementation of the grant is finally in high gear now that NeHII has completed the migration to their new platform. Here is an update on the grant activities:

- **Adding HL7 Data Sharing Participants.** One of the major components of our grant includes adding 18 Critical Access Hospitals and other facilities to NeHII as data sharing providers using HL7. Currently, 5 facilities have been implemented, 8 are in progress, and 3 more will begin implementation in a few weeks.

- **Implementing Population Health Analytics.** NeHII has also implemented Spectrum Population Health Analytics. Additional work needs to be done to map and standardize the data and then users at the five facilities funded through our grant will have access to this powerful tool.
- **Adding Direct Secure Messaging Users.** NeHII is working to add Direct Secure Messaging users at 50 long-term care and other facilities. 44 facilities have been confirmed and 14 facilities have been implemented. Recruiting facilities is hard, but implementation is easy.
- **Adding 5 C-CDA Data Sharing Participants.** NeHII will begin working with 5 health care providers to share data through C-CDA exchange as soon as NeHII's vendor, Optum, assigns a resource.
- **Sending Data between 5 Other Health Information Exchanges.** NeHIi is working on the legal agreements and will begin working on implementations soon.
- **Admission Discharge and Transfer Alerts via Mobile Messaging.** There is unfortunately not much demand for this service. Providers want to receive the messages using devices in their offices. This is a small part of our grant. We are talking to ONC about removing this project.
- **Sending Data from 8 Hospitals to the State's Syndromic Surveillance System.** One hospital (Community Hospital—McCook) has been implemented. St. Francis Memorial—West Point is in progress. Implementations on additional hospitals will start soon.
- **Working with Providers in 2 Rural Communities to Implement Health Information Exchange into their Workflow.** Project partners from UNMC with assistance from NeHII have been working with health care providers in Auburn and O'Neill to identify their needs, implement appropriate health information exchange technology, and to integrate the technology into their workflow. The project is going very well and generating interesting lessons learned. Training modules are also being developed to share information on the process and lessons learned.

EDUCATION COUNCIL REPORT

Tom Rolfes, Education IT Manager

Updates on Network Nebraska and Digital Education. Mr. Rolfes provided an update on the Network Nebraska and Digital Education strategic initiatives. Network Nebraska was deemed a closed project by the Technical Panel at their 8/9/2016 meeting. It has been, and continues to be, a successful project. There is more and more interest from community public libraries and municipalities to become participants. The Council, Collaborative Aggregation Partnership (CAP) and Network Nebraska Advisory Group (NNAG) continue to collaborate and recommend infrastructure options, as well as discuss network growth and reliability. Mr. Rolfes is working to develop a pilot project to determine the feasibility of using TV white space to extend the school campus information service to students in areas where connectivity is a challenge. Zoom videoconferencing is available through a statewide educational contract and has been beneficial to conduct the NNAG meetings. The next Education Council meeting will be held on April 10h at the Governor's Residence. Governor Ricketts and Ed Toner have been invited for an informal discussion with the Council.

GIS COUNCIL REPORT

Nathan Watermeier, State GIS Coordinator

Updates on Initiatives. Nathan Watermeier, GIS State Coordinator, announced his resignation to the Commissioners. His last day will be March 24. He thanked the Commission for their support of GIS and said it has been an honor to serve the State of Nebraska. In his new endeavor, he will still be involved with GIS and hopes to continue involvement with the State. With all that is occurring at the federal and state levels regarding Public Safety, Census 2020 and transportation, the past 5 years of the GIS Council has been about quality data, building standards and collaborative partnerships. Mr. Watermeier was presented with a certificate of appreciation for his dedication and time serving the State of Nebraska.

STATE GOVERNMENT COUNCIL REPORT

Update on CIO Roadmap. No report.

TECHNICAL PANEL REPORT

Walter Weir, Technical Panel Chair

2017-2019 Biennial Budget; Information Technology Project Proposals; November NITC Meeting Follow-up

Enterprise Project Designation for Dept. of Administrative Services - Enterprise Resource Management Consolidation*

Commissioner Weir provided a report on the Technical Panel review of this project at their meeting on February 14. The panel received an update on the project from Mr. Byron Diamond, DAS Director. This is a large project involving multiple systems which are used across state government. After the briefing, the Technical Panel voted unanimously to recommend that the project be designated as an enterprise project. Mr. Diamond agreed with the recommendation.

Commissioner Harvey moved to designate the Department of Administrative Services Enterprise Resource Management Consolidation Project as an enterprise project. Commissioner Spray seconded. Roll call vote: Greckel-Yes, Haack-Yes, Harvey-Yes, Meininger-Yes, Shundoff-Yes, Spray-Yes, and Weir-Yes. Results: Yes-7, No-0, Abstained-0. Motion carried.

Update on Dept. of Correctional Services-CIT [Corrections Information and Tracking system]

Commissioner Weir provided a report on the Technical Panel review of this project at their meeting on February 14. The panel received an update on the project from Mr. Ron TeBrink, IT Manager from the Department of Corrections. The agency has worked to better define the project beyond the limited information that was provided in their project proposal. The Technical Panel had no additional recommendations for this project.

Enterprise Projects; Project Status Dashboard

Commissioner Weir reviewed the project status dashboard report that was included in the meeting materials.

PRESENTATION ON BROADBAND IN NEBRASKA

Cullen Robbins, Nebraska Public Service Commission

Mr. Robbins began his presentation by connecting to the Public Service Commission's broadband map (broadbandmap.nebraska.gov) to show the state's coverage. The Public Service Commission is updating the map using data collected by the FCC from telecommunications providers as required by Section 706 of the Telecommunications Act of 1996. Broadband is supported by both the federal and state universal service funds. The universal service programs were originally developed to support telecommunications (voice) services. The FCC is modernizing the federal universal service fund to explicitly support broadband through the Connect America Fund. The PSC is also taking steps to modernize the Nebraska Universal Service Fund to explicitly support broadband. The Broadband Program provides support for broadband projects through a grant process. The Broadband Adoption Program funds broadband adoption activities. Another grant program, the Nebraska Internet Enhancement Fund, is funded through the leasing of dark fiber by public entities. Commissioners were given an opportunity to ask questions and have an informal discussion.

ADJOURNMENT

Commissioner Meininger moved to adjourn. Commissioner Greckel seconded. All were in favor. Motion carried.

The meeting was adjourned at 11:50 a.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by NITC staff.

Attachment 4-a

June 28, 2017

To: NITC Commissioners

From: Anne Byers

Subject: Community Council Report

New Member Nomination. The Community Council has nominated Timothy Lindahl from Wheat Belt Public Power to be a member of the Community Council. His resume can be found following this report. I will be asking you to approve his nomination.

Nebraska Broadband Today! The Nebraska Telecommunications Association is partnering with the Nebraska Broadband Initiative (Nebraska Public Service Commission, University of Nebraska, Nebraska Information Technology Commission, and Nebraska Library Commission) on the Nebraska Broadband Today conference which will be held on October 26 at the Cornhusker Marriott in Lincoln.

Nebraska Library Commission's Makerspace Grant. The Nebraska Library Commission, in partnership with the University of Nebraska-Lincoln, Nebraska Innovation Studio, Nebraska Extension, and Regional Library Systems, has received a $530,732 grant to from the Institute of Museum and Library Services (IMLS). The project, which will begin July 1, 2017 and conclude June 30, 2020, will work with 30 libraries to host traveling Library Innovation Studios (makerspaces) to stimulate creativity, innovation, and idea exchange to facilitate entrepreneurship, skill development, and local economic development. The deadline for the first application cycle is July 10, 2017.

Nebraska and the Digital Divide Index. Rural broadband and the Digital Divide is getting significant attention both nationally and within Nebraska. The *Digital Divide Index 2015* by Roberto Gallardo provided some interesting insights into broadband availability and adoption in Nebraska. Nebraska fares fairly well on socioeconomic indicators, ranking 21 out of the 50 states and District of Columbia and scores a not -great-but-respectable 35 on the composite index for both socioeconomic and infrastructure measures. However, the report ranks Nebraska 48th on infrastructure measures, ahead of only Mississippi, Montana, and Alaska.

The report also included state-level tables for further analysis. My analysis found:

- Broadband availability in Nebraska is improving. Broadband of at least 25 Mbps down and 3 Mbps up was available to 84.6% of Nebraskans in 2015, up from 79.3% in 2014.
- Average advertised download and upload speeds in Nebraska lag behind the United States and most neighboring states. Nebraska had an average advertised fixed download speed of 20.4 Mbps compared to the U.S average of 32.6 Mbps and an average advertised fixed upload speed of 8.5 Mbps compared to the U.S. average of 12.8 Mbps.
- There are significant differences in average upload and download speeds between the state's more populous and less populous counties. Nebraska counties with populations greater than 20,000 had an average advertised fixed download speed of 36.5 Mbps and an average advertised fixed upload speed of 16.2 Mbps. In comparison, Nebraska counties with populations

less than 20,000 had an average advertised fixed download speed of 16.8 Mbps and an average advertised fixed upload speed of 6.8 Mbps.

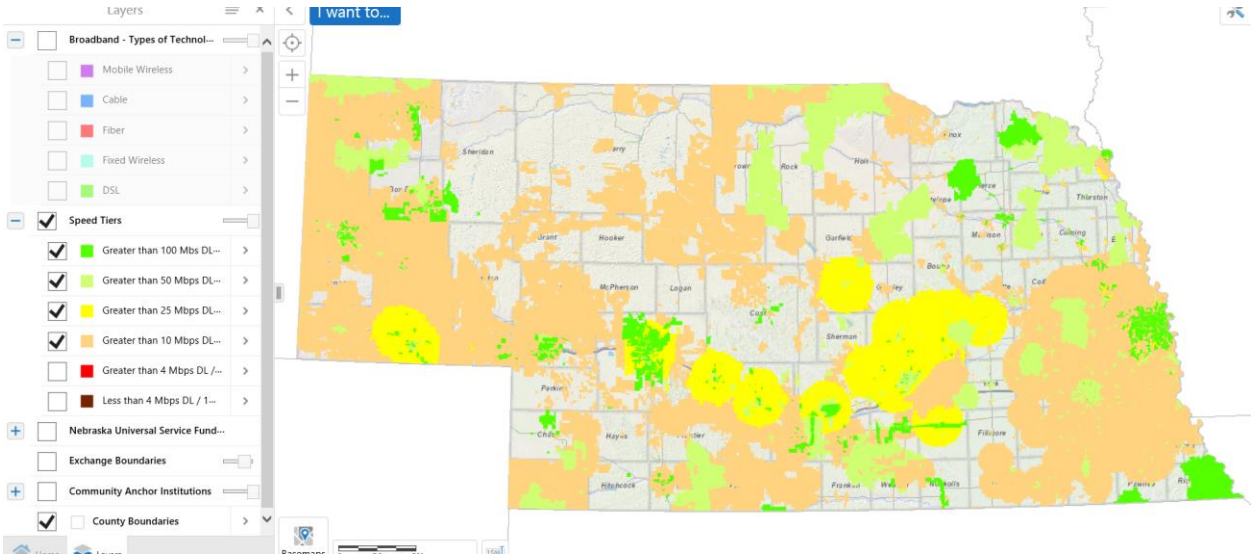
- Although the data seems to indicate that there is an urban-rural divide in Nebraska, this paints an overly simplistic picture of Nebraska. It is important to note that some rural counties performed quite well on several of the indicators. For example, Keith County with a population of 8,062 had the highest advertised upload and download speeds over in the state. Additionally, a look at the Nebraska Broadband Map shows fiber deployments in some very rural parts of Nebraska.
- Additionally, affordability and adoption of broadband at higher speed tiers—especially in some of the state's more rural counties—may be exacerbating the Digital Divide in Nebraska. Nebraska lags the U.S. and our neighboring states in the subscription rate to higher speed tiers of broadband (10 Mbps down and 3 Mbps up or greater). In half of the counties in Nebraska, fewer than 20% of households subscribe to broadband at speeds of 10 Mbps down and 1 Mbps up or greater.
- There are limitations to any method of ranking states. The Digital Divide Infrastructure Score was derived by first calculating county scores for broadband availability, average download speed, average upload speed, and subscription rates. The state score for each indicator was calculated by averaging the county scores. Using this method McPherson County which has no incorporated towns is given the same weight as Douglas County. This method provides a good picture of a measure across the geography of the state—but not the population of a state.

What can we do to help address this issue? Here are my recommendations:

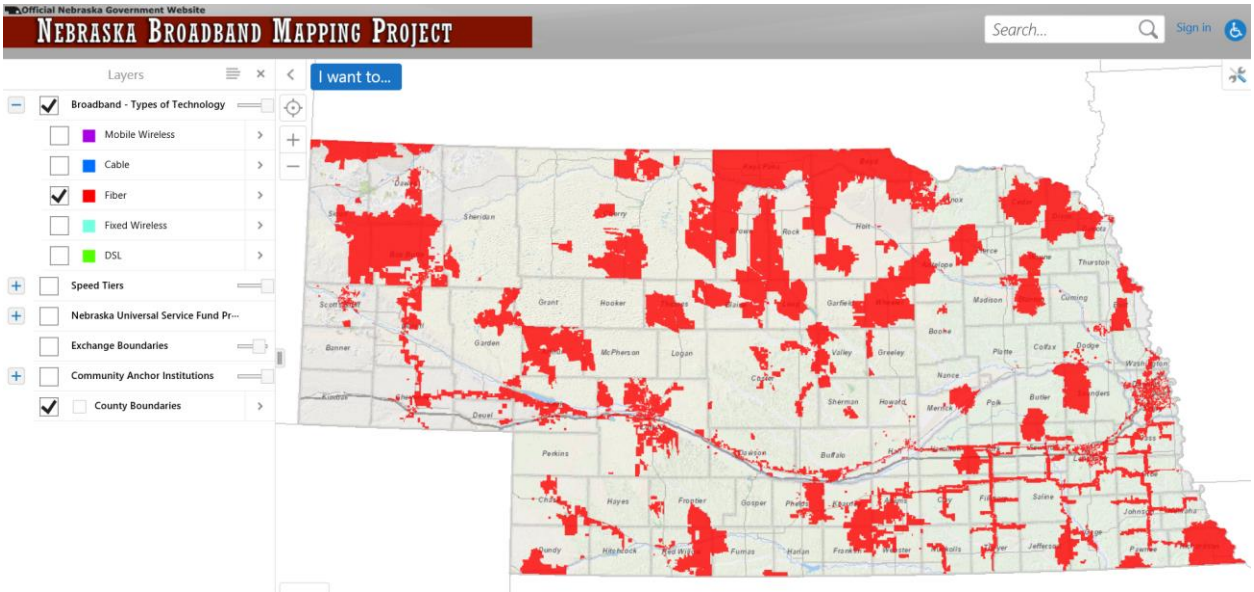
1. Bring attention to the issue. This article is a start.
2. Talk to broadband providers and officials in Nebraska in order to better understand factors impacting broadband deployment and adoption in Nebraska.
3. Talk to broadband providers and officials in other states to determine what strategies are being used to promote the deployment and adoption of broadband.
4. Support efforts to improve broadband access at public libraries. Libraries are an important access point in communities. Providing access at higher speed tiers in libraries can help area residents better understand the benefits of higher speed broadband. Libraries are also an important community asset to address the homework gap—the inequitable situation caused by most but not all students having broadband at home to complete homework.
5. Work with stakeholders in Nebraska to determine additional strategies and resources.

I am looking forward to hearing your comments and feedback. I have also included maps from the Nebraska Broadband Map showing broadband availability of at least 10 Mbps down and fiber deployments.

Broadband of at Least 10 Mbps Down Available



Fiber Deployments



Timothy J. Lindahl
Chief Executive Officer
Wheat Belt Public Power District
Sidney, NE 69162
Phone: 308-254-5871
E-Mail: tlindahl@wheatbelt.com

May 15, 2017

Nebraska Information Technology Commission
P.O. Box 95045
Lincoln, NE 68509

Dear Commission:
Thank you for your consideration of my desire to be a part of the Nebraska Information Technology Commission Community Council.

Technology and the ability to share information continue to play a more critical role in rural Nebraska. I see first-hand some of the handicaps we face in attracting business, attracting and retaining a younger workforce, adapting to a more complex agricultural industry, and utilizing economic efficiencies that IT can provide.

I started becoming engaged in technology back in high school, when I learned I could use the new technologies of the day to make my life easier. I learned quickly that technology could not only make my life better, but teaching others to utilize it made their lives better and more efficient. I was instrumental in forming a group of like-minded individuals to use our knowledge to help rural schools plan and implement technologies. We expanded to bring internet to rural Colorado in 1995. We also developed software tools to help rural Colorado businesses. In 2005, I took advantage of the opportunity to join the rural electric program and become an advocate for innovation and efficiency in this industry. Since that time, we have seen a great shift in the advancement of technology use to keep our rates stable, ultimately helping the rural economies we serve. With new technologies come new risks. My recent initiative has been educating the industry on cyber risks and strategic methods to address them. I have spoken at many conferences to many groups, offering my view of the tools that can mitigate these risks in a critical industry.

Rural America holds a large place in my heart and I wish to do whatever I can to help it succeed in this technology revolution. Being part of Wheat Belt Public Power, we are a critical part to many rural communities in Nebraska. Our core mission is to provide affordable and reliable energy, but with that, we have a strong vested interest in seeing our communities succeed. By being a part of this council, I see this as a conduit to lend our help, as an industry, to make lives better in Nebraska. I have included my resume for your contemplation. Please feel free to reach out if you wish to have any further discussion.

Sincerely,

Timothy J. Lindahl

Timothy J. Lindahl

Chief Executive Officer
Wheat Belt Public Power District
Sidney, NE 69162
Phone: 308-254-5871
E-Mail: tlindahl@wheatbelt.com

Professional Summary

A well-qualified and ambitious utility professional with 22 years of experience in executive management in the information technology and utility industries. Skilled at diplomatically and strategically implementing programs and improvements by establishing relationships and common vision to ensure business performance improvement, operational improvement, and cost stability. Leads teams and boards as a servant leader and with a cooperative approach that ultimately enables the organization to achieve high-level results. Holds human safety as a top objective.

Experience

2008–Current **Wheat Belt Public Power** Sidney, NE

General Manager and Chief Executive Officer

I report and am directly accountable to a seven-member board of directors for the management of a 5000+ meter rural public electric utility covering 3600 square miles in Nebraska. I have direct oversight of a 27 member staff and a $20 million budget. I have developed a long-term financial strategy, utilizing debt and innovation to optimize rate and financial efficiency for our owners. Our safety results are outstanding and we are operating well above our peers on most operational key ratios. I am very active in legislative, community, and technology issues. I have completed several technological improvements and maintained and improved our status of a top 20% national safety record in the rural electric industry, including no lost time incidents since 2008. A 2015 survey of our customers resulted in an overall satisfaction rating of 9.2 out of 10. My position allows me to participate on several boards and committees as noted later in this document.

2005–2008 **Wheat Belt Public Power** Sidney, NE

Information Technology Specialist

I was responsible for the development of the first technology and communications plan that included a build out of an IP network to all of our remote substations, and the plan to implement an Advanced Metering Infrastructure to every meter. I was able to work with our board for a long-term technology strategic plan. This provided us with a decision-making model that allowed for large gains in operational efficiency and investment.

1995–2005 **Power Technology Solutions Group, Inc**. Akron, CO

President and Co-Founder

I was a co-founder and led a technology group dedicated to brining technology and telecommunications to rural areas. We worked with schools and small businesses to help implement and utilize technology services. We continued to facilitate the development of a microwave broadband internet network for rural areas. We also developed customized web applications and stand-alone software packages for the agricultural industry as well as weather services, transportation companies, and state and local government agencies.

Education

2006-2007 University of Wisconsin Madison, WI

- National Rural Electric Cooperative Management Internship Program

1995 Concordia University Seward, NE

- B.A., Business Management with an Agricultural Economics emphasis through the University of Nebraska, Lincoln.

2005-2017

- Numerous NRECA, RMEL, CFC, and Safety related training courses on various topics

Boards/Committees

Current Boards and Committees

- National Rural Electric Cooperative Association Strategic Technology Advisory Council: 2011-Current
- National Rural Electric Cooperative Association Serve our Coop's Serve our Country Executive Task Force: 2015-Current
- Nebraska Workers Compensation Retention Committee: 2011-Current
- Nebraska Rural Electric Association Legislative Committee: 2013-Current
- Midwest Electric Consumers Association Water and Power Committee: 2009-Current
- Tri-State G&T Contract Review Committee: 2012-Current

Past Boards

- Tri-State G&T Managers Committee Chair: 2015-2016
- Basin Electric G&T Managers Advisory Committee (Representing Tri-State G&T): 2015-2016
- Nebraska Rural Electric Association Statewide Services Committee: 2011-2015
- Nebraska Rural Electric Association Managers Committee Chair: 2013-2014
- Nebraska Rural Electric Association, Executive Search and Transition Committee: 2012-2013
- Cheyenne County Nebraska Chamber of Commerce, Executive Search Committee, 2011
- Cheyenne County Nebraska Chamber of Commerce Government Relations and Advocacy Committee Chair: 2010-14
- Nebraska Rural Electric Association Policy and Resolutions Committee Chair: 2009-2013
- Cheyenne County Nebraska Chamber of Commerce President: 2012-2013
- Western United Electrical Supply Board of Directors (Representing Nebraska) 2010-2012
- Washington County Colorado Chamber of Commerce 1996-2005
- Power Technology Solutions Group, Inc. President 1995-2008

Timothy J. Lindahl
Chief Executive Officer
Wheat Belt Public Power District
Sidney, NE 69162
Phone: 308-254-5871
E-Mail: tlindahl@wheatbelt.com

May 15, 2017

Key Items and Projects

System

Meters	5056
Service Area	3600 sq. miles
Miles of Line	2,522
Meters Per Mile	1.97
Revenue	$19.2M
Booked Plant	$52.7M
kW Peak	62MW
kWh	176M
FT Employees	27
Board Members	7
G&Ts	Tri-State, Basin, WAPA

Financial Performance (2015)

Cost of Power	73.88 mills
Cost of Power % of budget	67.47%
TIER	12.66
MDSC	1.97
Blended Interest on LTD	1.17%
Equity	83.76%
Controllable Expenses	24.94 mills

Safety

Last Lost Time Accident (twisted ankle)
2008

OSHA Recordable Incidents 2014
0, 1 minor in 2015, 2016 0

Workers Compensation Experience Mod
.760 (below .85 since 2008)

NRECA Safety Achievement

Top 20% Safety Performing Rural System

Timothy J. Lindahl
Chief Executive Officer
Wheat Belt Public Power District
Sidney, NE 69162
Phone: 308-254-5871
E-Mail: tlindahl@wheatbelt.com

Recent Major Projects

The following recent projects were completed or are in progress under my leadership, however, there are many people involved with these projects that deserve the credit for making them happen.

2015-Negotiated a no-cost project with RFD-TV to run rotating two-minute stories on farm and general electrical safety for a six-month period.

2015-2016-Launched a new annual statewide Information and Technology conference to deal collectively with utility cyber security and other IT needs in the state of Nebraska. Held in April 2016.

2016-Instramental in forming a G&T Technology Advisory Council at Tri-State G&T to collectively deal with Energy Technology and Cyber Security issues within the membership, held first Cyber Conference in October 2016.

2015-2016- Developed a plan and implemented the construction of a new $6M headquarters campus with $0 rate impact. Completed the move in May, 2016.

2014-2015- Facilitated the initiation of the Touchstone Energy's Service Excellence program for the team.

2008-2017-Developed a long-term financial forecasting tool, integrating an optimal debt structure to fine tune revenue requirements and mitigate load loss and upward rate pressure.

2014-Ongoing-Developed a risk management plan that included a plant replacement plan, aligned with a long-term financial forecast and aging infrastructure to boost reliability through increased redundancy and aging infrastructure replacement.

2015-2017-Spoke on strategic Cyber Security issues to boards of directors and senior staff at the 2015 and 2016 NRECA Region 7 & 9 meetings, both in the general sessions and breakout sessions, 2016 and 2017 NRECA CEO Conferences, 2016 Touchstone Energy's New and Emerging Technologies Conference, 2016 Nebraska Rural Electric IT Conference, and the 2016 Midwest Electric Consumers Annual Meeting. I led a workshop in January 2017 on engaging Boards of Directors and Senior Management on Strategic Risk Management in Cyber Security for NRECA and the Department of Energy at the National Renewable Energy Laboratory. Have lined up to lead workshops in 2017 for HR professionals on creating a cyber and physical security culture for NRECA. Contributed to articles in RE Magazine and our Statewide magazine on Technology and Security Issues.

2015-2016-Participated in a community based broadband internet working group to determine optimum solutions to provide broadband services to the communities that we serve.

2016-Participated in a Target Market Strategy Study for our community to mitigate effects of an industrial downturn and to find opportunities for the Bass Pro/Cabela's acquisition.

2008- Implemented an Advanced Metering Infrastructure (AMI) project to every meter and a long-term plan to continue the transition to new technology AMI over time with continued investment returns.

2008-2017-Implemented strategic tools and improved processes which allowed for a 10% reduction in workforce through attrition while re-aligning existing team members with job duties that matched their strengths and our needs.

2016-2017-We were approached by and are currently negotiating an agreement with a city in our territory to serve their wholesale and/or retail electric needs.

2008-2017-Developed close working relationships with our local, state, and federal elected officials, including consistent communication on key issues.

Attachment 4-b

June 29, 2017

To: NITC Commissioners

From: Anne Byers

Subject: eHealth Council Report

ONC Grant Update

Nearly two years ago, the NITC received a $2.7 million grant from the U.S. Department of Health and Human Services Office of the National Coordinator for Health IT (ONC). The grant got off to a slow start due to challenges with recruiting health care providers and NeHII's move to a new health information exchange (HIE) platform. The grant is now in high gear as NeHII works to implement as many facilities as possible by July 26, 2017. While we will not meet all of our targets, ONC is pleased with our progress to date.

Implementing health information exchange isn't easy. Barriers and challenges include costs, interoperability issues, and time and resource limitations of the health information exchange, participating facilities, the health information exchange vendor, and the Electronic Health Record vendors of participating facilities.

The cost to participating facilities is one of the greatest barriers. NeHII's new pricing model makes participation more affordable for Critical Access Hospitals and has led to increased interest from these small hospitals. The grant covers implementation costs which further addresses the cost barrier.

Here is a summary of the grant progress as of June 29. I will provide an update prior to the NITC meeting.

- **Adding HL7 Data Sharing Participants.** One of the major components of our grant includes adding 19 Critical Access Hospitals and other facilities to NeHII as data sharing providers using HL7. Currently, 12 facilities have been implemented, 3 are scheduled to go live the week of July 10, and 8 more are starting implementation. We could possibly have up to 22 or 23 implementations.
- **Implementing Population Health Analytics.** NeHII has also is also implementing Spectrum Population Health Analytics for five facilities. Nemaha County Hospital, Mary Lanning Health Care are in the process of provisioning users and validating data. NeHII is working to identify two additional participants.
- **Adding Direct Secure Messaging Users.** NeHII had set a goal to add Direct Secure Messaging users at 50 long-term care and other facilities. 14 facilities have been implemented. Recruiting facilities is hard, but implementation is easy.
- **Adding 5 C-CDA Data Sharing Participants.** Work is underway with 3 health care providers--CHI Health-TPN Clinics, Think Whole Person Healthcare, and Family Practice of Grand Island. Montgomery County clinic in Red Oak, IA is in progress. Some technical issues with sending the SAML token for secure transport were encountered with the Grand Island Clinic.
- **Sending Data between 5 Other Health Information Exchanges.** Work with the Kansas Health Information Network (KHIN) and Missouri Health Connect is in progress. Unity Point in Iowa is also moving ahead.

- **Admission Discharge and Transfer Alerts via Mobile Messaging.** There is unfortunately not much demand for this service. Providers want to receive the messages using devices in their offices. This is a small part of our grant. We have removed this project.
- **Sending Data from 8 Hospitals to the State's Syndromic Surveillance System.** Two hospitals--Community Hospital in McCook and St. Francis Memorial in West Point--have been implemented. Children's Hospital is in progress. Johnson County Hospital is scheduled to start soon.

- **Working with Providers in 2 Rural Communities to Implement Health Information Exchange into their Workflow.** Project partners from UNMC with assistance from NeHII have been working with health care providers in Auburn and O'Neill to identify their needs, implement appropriate health information exchange technology, and to integrate the technology into their workflow. The project is going very well and generating interesting lessons learned. Training modules are also being developed to share information on the process and lessons learned.

- **Increasing Consumer Awareness**. A consumer awareness campaign including newspaper, radio, billboards, and social media is kicking off.

Lessons Learned

Recruitment and Engagement of Long-Term Care and Post-Acute Care Facilities (LTPACs) and Critical Access Hospitals (CAHs)

- It takes a lot of work to engage Critical Access Hospitals and long-term and post-acute care facilities.
    - The biggest barrier to health information exchange remains cost, including interfaces fees from the electronic health record vendors of hospitals, clinics, long-term and post-acute care facilities, and other health care providers.

Better Understanding the Needs of Long-Term and Post-Acute Care Facilities

- Work on the Integrated Community project has helped us better understand the needs of long-term and post-acute care facilities and the importance of including long-term care and post-acute care facilities and others providers in the health information exchange. Through the grant, the team has developed several use cases for exchanging health information with long-term and post-acute care facilities. Demonstrating the value of different use cases will facilitate efforts to engage long-term and post-acute care facilities.

Integration of Health Information Exchange into the Provider Workflow

- The process developed for the Integrated Communities Project is proving to be useful in engaging providers and helping them integrate health information exchange into their workflow.
    - The process started by bringing together providers within a community, including the hospital, clinic(s), pharmacy, and long-term and post-acute care facilities, to discuss their interest in sharing health information and to kick off the process.
    - The facilitators/workflow integration specialists from UNMC set up follow-up meetings with providers to identify what health information was needed from other health care providers.
    - With technical assistance from a NeHII project manager, the appropriate technologies for exchanging health information exchange were matched to each use case.

- The team worked with facilities to prioritize use cases.
- The team then worked with facilities to implement the appropriate technologies, test the technologies, evaluate the quality and timeliness of the information sent and received, and integrate the new process into the provider workflow.

- The process works best when a local health care provider acts as a community champion, encouraging community health care providers to participate in the progress.
- Having a facilitator to start the engagement process is another key component. It was also very helpful to have a project manager from NeHII as part of the team to provide technical assistance.
- Having all participating providers set up with both Direct and query-based exchange early in the process allows for the implementation of a greater number of use cases.
- Health information exchange isn't plug and play. It takes time and effort to integrate health information exchange into the provider workflow. For example, the NeHII Community Patient Profile (CPP) is easy to implement, but usage doesn't usually take off unless the CPP can be accessed with single sign on from the electronic health record. Direct has been touted as an easy first step for health information exchange, but in reality it takes time and effort to identify use cases and to work with other health care providers to begin exchanging information.

eHealth Council

The eHealth Council met on April 5 from 1:30 to 4:00 at the 1526 Building in Lincoln.

NeHII Annual Meeting

Nebraska Health care providers and policy makers are invited to attend the NeHII Annual Meeting on August 3 at the Younes Conference Center in Kearney. Dr. Donald Rucker, the National Coordinator for Health IT will be the keynote speaker. A panel of participants from the Auburn Integrated Community project will also share their experiences and lessons learned.

Prescription Drug Monitoring Program (PDMP) Update

The Nebraska Prescription Drug Monitoring Program (PDMP) is a statewide tool that collects dispensed prescription information and is housed on the NeHII Health Information Exchange platform. The Nebraska PDMP focuses on patient safety.

Nebraska's PDMP was originally established in 2011 (Neb. Rev. Stat. §§ 71-2454, 71-2455, 71-2456). LB 471 in 2016 provided additional structure to the PDMP. It requires all dispensed controlled substances to be submitted on a daily basis to the PDMP as of Jan 1, 2017. Starting January 1, 2018, all dispensed prescriptions will be reported to the PDMP. The PDMP stores the information in a secure database and makes it available to healthcare professionals as authorized by law.

Further legislation (LB 223) passed in 2017 allows licensed or registered health care professionals to be designated by a prescriber or dispenser to act as an agent for the purpose of submitting or accessing

data in the PDMP. The legislation also mandates user training.

The Department of Health and Human Services received two grants which are supporting efforts to develop a PDMP and to prevent prescription drug overdoses.

The Harold Rogers-DOJ Bureau of Justice Assistance grant is supporting PMPD training and PDMP software enhancement. PDMP trainings are being conducted through live webinars, on-demand webinars (went live in March), in-person sessions and downloadable tutorials. Approximately 900 dispensers and prescribers have been trained since December.

The Prescription Drug Overdose Prevention for States Grant (PDO-PfS) — CDC grant is supporting the following three strategies:

- Develop and implement pain management guidelines.
- Conduct needs assessment and educate on expanded access to naloxone.
- Enhance and maximize the Nebraska PDMP system.

The PDMP team is working to increase access and use of the PDMP by medical professionals. Over 3,500 prescribers and 1,300 dispensers have registered as users. 100% of total eligible Nebraska dispensers have registered to report to the PDMP or have been exempted for the 2017 year. This includes community pharmacies, dispensing practitioners, and long-term care automated pharmacy dispensers. 82%% of total eligible mail service pharmacies have registered to report to the PDMP or have been exempted. The grant is also supporting enhancements to utilize PDMP data for public health surveillance.

Additionally, Nebraska's Department of Health and Human Services received a $2 million grant from the Substance Abuse and Mental Health Services Administration (SAMHSA) for opioid response in June 2017. The grant, awarded to the Division of Behavioral Health, may be renewed in 2018 for the same amount. SAMHSA's Center for Substance Abuse Treatment and Center for Substance Abuse Prevention will fund Nebraska's 2017 State Targeted Response to the Opioid Crisis Grant. The program aims to address the opioid crisis by increasing access to treatment, reducing unmet treatment need, and reducing opioid overdose related deaths through the provision of prevention, treatment and recovery activities for opioid use disorder (including prescription opioids as well as illicit drugs such as heroin.)

Attachment 4-c

Nebraska Information Technology Commission
EDUCATION COUNCIL

2017-19 Membership Renewals/Replacements EXPIRING June 30, 2017

Name	Representing	Status
	HIGHER EDUCATION (2017-19 term)	
Mark Askren	UN System	**Hank Bounds confirmed (6/21/17)**
Mike Carpenter	Independent Colleges & Universities	**Maryanne Stevens confirmed (6/28/17)**
Derek Bierman	Community College System	**Greg Adams confirmed (6/22/17)**
Steve Hotovy	State College System	**Stan Carpenter confirmed (6/21/17)**
	K-12 EDUCATION (2017-19 term)	
Dr. Ted DeTurk	Educational Service Units	**Dave Ludwig confirmed (6/23/17)**
Dr. Mike Lucas	Administrators	**Mike Dulaney confirmed (X/X/17)**
Stephen Hamersky	Private Education	**John Perkinton confirmed (6/21/17)**
Matt Chrisman	Public Teachers	**Nancy Fulton confirmed (6/22/17)**

Note
Underlined Candidates are new voting members to the NITC Education Council and have a brief biographical statement attached to this document

RECOGNITION

NITC Strategic Initiatives Status Report (07/12/2017)

Strategic Initiative, Action Item and Deliverable/Target

Network Nebraska (Education Council)		Status	Notes
1	**Prepare for the future of Network Nebraska**		
1.1	Develop strategy to accommodate community affiliate connections	Completed	Internet2/IMLS grant provided a technology toolkit and funded OCIO and Nebraska Library Commission staff travel to 5 rural libraries during the month of March: Wymore, Valley, Walthill, Atkinson, Gering. Network Nebraska subcommittee met to discuss this action item on 6/29/2017.
1.2	Use automated tools to monitor network uptime and web depiction	In progress	Further development in progress.
1.3	Implement incident management and change control frameworks	In progress	External communication about outages and maintenance has improved.
1.4	NNAG & CAP to guide OCIO decisions about network growth/reliability	In progress	CAP and NNAG continue to collaborate and recommend infrastructure options. Three longhaul backbone contracts were awarded and new circuits purchased for 7/1/2017, with a 51% overall reduction in cost.
1.5	Review and update security services and practices and strategize future services	In progress	Distributed Denial of Service (DDoS) solutions are being tested and enterprise Internet2 DDoS solution is being considered for purchase.
2	**Serve as the communication hub for new and existing Participants**		
2.1	Develop and implement a communications strategy	In progress	Draft Executive Briefs for different target audiences were reviewed and discussed on 6/29/2017.
2.2	Conduct an annual services survey of all Participants to guide service development	In progress	Subcommittee has formed to discuss this Action Item.

NITC Strategic Initiatives Status Report (07/12/2017)			
Strategic Initiative, Action Item and Deliverable/Target			
Digital Education (Education Council)		**Status**	**Notes**
1	**Create professional development opportunities for Nebraska educators**		
1.1	Establish multimodal, virtual communities of practice for all levels of educators	In progress	Initial inventory of professional development opportunities was gathered on 8/17/2016.
2	**Address students' technical challenges in high school to college transition**		
2.1	Conduct a research project to identify existing infrastructure and pedagogy efforts	In progress	EC subcommittee met on 2/15/2017 to discuss this action item.
2.2	Identify opportunities for collaboration to ease student transition to college	In progress	EC subcommittee met on 2/15/2017 to discuss this action item.
2.3	Identify key challenges for transitioning students and mitigate the challenges	In progress	EC subcommittee met on 2/15/2017 to discuss this action item.
2.4	Create an effective practices guide for using flexible learning technologies	In progress	EC subcommittee met on 2/15/2017 to discuss this action item.
2.5	Develop a strategy to encourage vendors to implement data exchange standards	In progress	NDE I.T. Project Proposal 13-01 addresses this action item.
3	**Address the need for equity of access as it relates to digital education**		
3.1	Form a joint study group to identify opportunities/actions to ensure equitable access	In progress	Community Council and Education Council study group have met four times to consider options to achieve equity of access and digital inclusion. An Equity of Access essay was published in the NETA Newsletter and the state broadband newsletter.
3.2	Work with other stakeholders to ensure equitable Internet access for all students	In progress	Beatrice Public Libraries was awarded a $15,000 IMLS TV White Space grant from the Gigabit Libraries Network and San Jose State University. They will be working with Beatrice Public Schools and ESU 5 to implement. Chadron Public Schools and Chadron Public Library have begun to collaborate on a shared Internet augmentation project.
3.3	Identify and promote accessible products and services to achieve equitable access	In progress	Dr. Christy Horn, NU accessibility expert, presented at the 12/21/2016 EC meeting.

Network Nebraska-Education Report
June 30, 2017

2016-17	2017-18 (projected)
PARTICIPATION	
Participants: 291	Participants: 292 (up .3%)
Added: +1 public library, +1 private school, +1 judicial school district, +1 municipality, -.75 parochial school	Adding: +.25 public library, +.25 municipality, +.25 nonprofit educational services provider, +.25 nonprofit educational content provider
PARTICIPATION FEE	
1.0 Participation Fee: $217.47/month	1.0 Participation Fee: $217.06/month
.25 Participation Fee: $ 54.37/month	.25 Participation Fee: $ 54.27/month
INTERREGIONAL TRANSPORT FEE	
1.0 Interregional Transport Fee (K-12): $21.49/month	1.0 Interregional Transport Fee (K-12): $17.72/month (- 17.5%)
.25 Interregional Transport Fee (K-12): $ 5.37/month	.25 Interregional Transport Fee (K-12): $4.43/month
Interregional Transport Fee (H.E.): $67.16	Interregional Transport Fee (H.E.): $53.70 (- 20.0%)
INTERNET ACCESS	
Internet Unit Cost (K-12): $.2432/Mbps/month	Internet Unit Cost (K-12): $.2662/Mbps/month
Internet Unit Cost (H.E.): $.7920/Mbps/month	Internet Unit Cost (H.E.): $.8066/Mbps/month
Commercial Peering Surcharge: $ .0349/Mbps/month	Commercial Peering Surcharge: $ .0405/Mbps/month
Total Commodity Internet Ordered: 47.56Gbps	Total Commodity Internet Ordered: 56.82Gbps (+ 19.5%)
Total Commodity Internet Purchased: 30.0Gbps	Total Commodity Internet Purchased: 35.0Gbps (+ 16.7%)
Total Peering Services Purchased: 23.0Gbps	Total Peering Services Purchased: 44.0Gbps (+ 91.3%)
ZOOM VIDEOCONFERENCING	
Purchased Licenses: 13,750	Purchased Licenses: 20,000
Revenue: $31,991.00	Revenue: $91,000.00
Expenses: $30,000.00	Expenses: $90,000.00

Attachment 4-d

June 21, 2017

To: NITC Commissioners

From: John Watermolen, State GIS Coordinator
Jon Kraai, Chair, GIS Council
Sudhir Ponnappan, Vice-Chair, GIS Council
Tim Cielocha, Past-Chair, GIS Council

Subject: GIS Council Report

Nebraska Spatial Data Infrastructure (NESDI) Updates

Nebraska Statewide Imagery Program

Statewide Imagery Program-Business Plan: The GIS Council approved the Statewide Imagery Program business plan. The business plan provides for a sustainable statewide imagery program, that facilitates the acquisition, historic preservation, maintenance and distribution of high quality digital imagery products to various government agencies and the public. I request that the Commission, please approve this business plan, so we can work to acquire imagery starting next spring. A summary of the business plan and the actual business plan is provided with these notes as an attachment. The core product involves a statewide orthoimage with a minimum spatial resolution of twelve inches meeting state imagery standards. The estimated average cost for this imagery layer is $1.78 million. Document is Appendix 1

Administrative and Political Boundaries

A new Administrative and Political Boundary Working Group has formed and has met several time since. A list of all the commonly used boundaries were documented so they could be prioritized on which ones to start assessing for attribution and geometric placement. The group is in the process of classification of the different data sets for the appropriate categories. The boundaries that were prioritized included municipalities, counties, and emergency service zones. Many other boundaries are dependent on these core boundaries. Some of the core boundaries are predicated on NESDI data layers such as street centerlines and parcels. The geometric placement will be important to address between data layers before finalizing the final placement of administrative and political boundaries.

Several working group members have been tasked to take lead on researching and identifying data for these layers. Items such as legal descriptions, statutes and laws, data stewardship, and metadata will be documented through the assessment phase of the program.

Nebraska Street Centerline and Address Program

The Street Centerline and Address working group has identified goals and objectives for the draft business plan. The goal is to develop and maintain a seamless statewide street centerline and point address referencing program for Nebraska. This involves developing and maintaining statewide geodatabases that provides map coordinates for the centerlines of all the state's highways, streets, and roads, along with their associated names and address ranges. In addition, this program will provide a statewide point address geodatabase representing discrete point locations that contains detailed

information such as physical address, parcel information, and other detailed information necessary for state needs.

The following are specific objectives for the program.

1. Establish a program management team and operations plan with administrative coordination from the Geographic Information Office, Nebraska Department of Roads, and Public Service Commission.
2. Establish and maintain standards, policies and strategies to emphasize cooperation and coordination among state, municipalities, county, and federal stewards.
3. Develop implementation and maintenance workflow roles and responsibilities for statewide aggregation and data exchanges between data stewards and the Geographic Information Office, Nebraska Department of Roads, and Public Service Commission.
4. Identify and develop funding sources for program implementation and long term sustainability.
5. Implement procurement and vendor selection processes for product and services, if or where needed, to support the development and maintenance of street centerline address databases and overall network.
6. Develop and maintain the Nebraska Street Centerline Database (NSCD) and the Nebraska Address Database (NAD) including related geocoding, routing, and other networking datasets and map services.
7. Expand existing data sharing and distribution methods to leverage databases and the network so they are accessible, both publicly and for secure uses.
8. Provide communications, technical assistance and education outreach activities supporting the efficient utilization of databases and the network.
9. Conduct an annual evaluation and make necessary programmatic adjustments to standards, and other processes that impact activities and outcomes of the program.

The assembly of current address data through the Nebraska Address Database (NAD) continues within the OCIO Geographic Information Office. More than twelve counties and other state datasets have started to be compiled and incorporated into the standardized geodatabase.

<u>Nebraska Statewide Elevation Program</u>

Collection is complete and on schedule with the dates in the USGS agreement documents. The Sandhills data is due to USGS for review at the end of December with final delivery as February 28, 2018. The Hat Creek-White River area is due to USGS September 1 and final delivery to NRCS on Dec 30, 2017. The South Platte Basin data has been delivered and is having some post processing done by DNR before public consumption.

OCIO Geospatial/GIS Enterprise

Public Service Commission Agreement: OCIO and the Public Service Commission entered into an agreement to provide an updated repository and a web based map viewer to collect data for next generation 911 (NG-911). The development cost was $9,194.50 and an annual maintenance cost of $5,656.80. OCIO was able to support this through the services that it provides and saved the Public Service Commission a total of $74,148.70 (development and maintenance) based on the cost of the original GIS repository created in 2006. PSC received a quote from a vendor to provide a similar product at a development cost of $47,674 and an annual maintenance cost of $299,000 (which did provide for built in QA/QC functions)

Agency GIS Consolidation/Integration: Department of Roads/Transportation- Consolidation and Integration- This is an ongoing process. We are making progress. There have been some setbacks along the way and institutional knowledge lost because of retirements and resignations. The challenges are more institutional because programs lived in silos, but I feel confident that the team NDOT(R) has put together and the steps they are taking like inventorying data sets and wanting to hire a GIS manager for the agency. These steps along with guidance from OCIO, I feel that we will continue to make progress with this consolidation and will provide a foundation for other agencies, when we work with them to consolidate.

ESRI- GIS License Consolidation: All of the state agencies use the ESRI ARCGIS platform in some capacity for GIS mapping, analysis. Currently every agency has a customer number and manages their own licenses with various renewal dates. Our goal is to consolidate all desktop and server licenses to 1 account that will provide for a consistent management of the license and ways to find cost savings. By doing this will help the state be able to address the migration to a named user licensing structure. It can help the state determine if we would want to pursue an Enterprise Licensing Agreement with ESRI for their products, and services. Since the ARCGIS is a platform that includes web mapping capabilities and not just software, this could be a hurdle we may have to encounter. Currently with each agencies ESRI licensing, they are entitled to an ArcGIS Online Account. This web based mapping and analysis tool is being used in various degrees by the agencies and with some has become part of their online identity. If ESRI will allow the state to consolidate the software licenses into 1 account and leave the ArcGIS Online Account available to each agency, then I see this effort being very successful. If ESRI will not allow it, then we will have to look into other options because migrating all the agencies who are leveraging ArcGIS Online into 1 account would be an enormous cost of time and resources and would need to address security issues in the process.

Nebraska Spatial Data Infrastructure (NESDI) Status Report

Report Date: June 21, 2017

NITC Strategic Initiatives Status Report			
Strategic Initiative, Action Item and Deliverable Target		Status	Notes
Nebraska Spatial Data Infrastructure (NESDI)			
1	Formalize the definition of the Nebraska Spatial Data Infrastructure (NESDI) and data stewardship		
1.1	Establish an ad hoc committee of GIS Council representatives	Completed	
1.2	Develop a document that defines the NESDI and the role of data stewardship	In Progress	The definition for the NESDI and data stewardship has drafted. Priority is on developing and implementing other NESDI business plans and then provide resource information back to this document.
2	Geodetic and Survey Control Inventory and Assessment		
2.1	Establish an ad hoc committee involving stakeholders from government, private industry and the survey community	Completed	
2.2	Develop a current inventory and assessment report of geodetic and survey control	In Progress	A partnership has begun with the U.S. Interior Bureau of Land Management to share our localized data to help improve the state's PLSS data layer. Localized data continues to populate our new PLSS database. An interactive map viewer has been created to support geodetic and survey control data for the Public Land Survey System (PLSS) – http://maps.nebraska.gov/nemap/PLSS This map viewer provides access to data submitted on behalf of the Low Distortion Projection Project.
3	Nebraska Statewide Elevation Program		
3.1	Establish an Elevation Working Group	Completed	
3.2	Identify standard elevation product(s) and develop a set of standards	Completed	Developed and adopted on October 28, 2014
3.3	Develop a business plan	Completed	Developed and approved on March 26, 2015

3.4	Implement the program	In Progress	Collection is complete and on schedule with the dates in the USGS agreement documents. The Sandhills data is due to USGS for review at the end of December with final delivery as February 28, 2018. The Hat Creek-White River area is due to USGS September 1 and final delivery to NRCS on Dec 30, 2017. The South Platte Basin data has been delivered and is having some post processing done by DNR before public consumption.
4	Nebraska Statewide Imagery Program		
4.1	Establish an Imagery Working Group	Completed	
4.2	Identify standard imagery product(s) and develop a set of standards	Completed	Developed and adopted on October 28, 2014
4.3	Develop a business plan	In Progress	Developed and adopted on February 15, 2017
4.4	Implement the program	Not Started	
5	Street Centerline-Address Database		
5.1	Establish a Street Centerline and Address Working Group	Completed	The slate of working group members have been extended to involve representatives from the Public Service Commission. There is a core working team that meets on a weekly basis since December.
5.2	Identify standard street centerline and address product(s) and develop a set of standards	Completed	Developed and adopted on March 27, 2015
5.3	Develop a business plan	In Progress	Goals and objectives have been drafted for the business plan. The necessary steps for implementing the program is currently being planned and documented into the business plan. Existing street centerline and address data are being assessed for completeness and quality so that future needs are also included in the business plan.
5.4	Implement the program	In Progress	The OCIO Geographic Information Office has begun to accumulate address points to populate the Nebraska Address Database (NAD).
6	Statewide Land Record Information System		
6.1	Establish a Land Records Working Group	Completed	
6.2	Update the current NITC 3-202 Land Record and Information Mapping Standards	In Progress	Original standards adopted on January 27, 2006 and amended on March 1, 2011.

6.3	Develop a Nebraska Statewide Parcel Geodatabase Development and Maintenance Plan	Completed	Developed and approved on May 27, 2015
6.4	Implement the program	In Progress	A request for parcel data was submitted to assessors in December 2016. Parcel data was started to be combined in the Nebraska Statewide Parcel Geodatabase in January. Data is coming in much slower than anticipated, in addition missing information that we have requested through the process.
7	NebraskaMAP - A Geospatial Data Sharing and Web Services Network		
7.1	Establish a NebraskaMAP Working Group	Completed	
7.2	Develop NebraskaMAP Geospatial Data Sharing and Web Services Network Business Plan	In Progress	The business plan has been modified for inclusion within the State of Nebraska Geospatial/GIS Enterprise and OCIO Roadmap initiatives.
7.3	Develop and implement NebraskaMAP data clearinghouse enterprise platform	In Progress	Data continues to be updated and submitted through NebraskaMAP. A new addition to the clearinghouse is a secure repository to handle the GIS 911 data sets for Nebraska. This was developed in December and implemented in January.

APPENDIX 1

NEBRASKA STATEWIDE IMAGERY PROGRAM

Business Plan

"Produce a sustainable statewide imagery program for the state that facilitates the acquisition, historical preservation, maintenance, and distribution of high quality digital imagery products to be utilized through various governmental uses and for public consumption."

Approved: February 15, 2017

NEBRASKA INFORMATION TECHNOLOGY COMMISSION GIS COUNCIL
AND
OFFICE OF THE CHIEF INFORMATION OFFICER

TABLE OF CONTENTS

Foreword **3**

Acknowledgements **3**

Executive Summary **4**

1.0 Program Justification **5**

1.1 Program Needs 5

1.2 Strategic Foundation for a Business Plan 7

2.0 Goals and Objectives **8**

2.1 Goals 8

2.2 Program Objectives 8

3.0 Benefits **9**

3.1 Anticipated Benefits 9

3.2 Return on Investment and Shared Value 11

4.0 Background **12**

4.1 Remote Sensing 101 and the Context of Products in this Business Plan 12

4.2 History of Nebraska's Imagery 13

4.3 Imagery for the Nation 14

5.0 Program Requirements **14**

5.1 Organizational Structure 15

5.2 Legislative Support 16

5.3 Data, Application and Product Components 17

5.4 Standards 19

5.5 Technology Requirements 21

5.6 Human Resource Requirements 22

5.7 Costs 23

5.8 Finance and Procurement Strategy 25

5.9 Reduction of Risk 28

6.0 Implementation Plan **29**

6.1 Implementation Details and Timeline 29

7.0 Communications and Outreach **35**

7.1 Communications 35

7.2 Technical Assistance and Education Outreach 35

8.0 Measuring Success and Feedback for Recalibration **36**

9.0 References **37**

Appendix I - Relationship of Imagery to other Nebraska Spatial Data Infrastructure Layers **38**

Appendix II - Orthoimagery Applications and Feature Recognition Examples by Resolution **39**

Appendix III - Implementation Timeline **40**

Foreword

This business plan was coordinated through the Nebraska Information Technology Commission (NITC) GIS Council. Administrative and staff support was provided through the Geographic Information Office within the State of Nebraska, Office of the Chief Information Officer (OCIO). This plan follows national guidelines of the Federal Geographic Data Committee (FGDC) Fifty States Initiative, Cooperative Agreements Program (CAP). The Fifty States Initiative is a joint effort between FGDC and the National States Geographic Information Council (NSGIC) to advance the National Spatial Data Infrastructure (NSDI) through planning and coordination of diverse stakeholders involved with geospatial data, applications and services.

Acknowledgements

The resources and information for the plan could not be possible without the leadership of the Imagery Working Group. This working group was chartered to gather input, discuss and help create the business plan. Various industry and other state partners were solicited for information and summarized within this plan. This business plan coordination and writing was led by Nathan Watermeier, NITC Administrative Manager with the State of Nebraska, OCIO.

Mike Schonlau, Spokesperson, City of Omaha/Douglas County
Nathan Watermeier, Geographic Information Office/OCIO/NITC
Marsha Munter, Nebraska Department of Roads
Bill Wehling, Nebraska Department of Roads
Rob Christian, Nebraska Department of Roads
Michael Niedermeyer, Nebraska Department of Roads
Josh Lear, Department of Natural Resources
Amy Zoller, Department of Natural Resources
Craig Romary, Nebraska Department of Agriculture
Les Howard, UNL Conservation and Survey Division
Milda Vaitkus, UNL School of Natural Resources
James Langtry, USGS
Billie Jo Smith, USDA FSA
Eric Herbert, Sarpy County
Jeff McReynolds, City of Lincoln/Lancaster County
Tim Cielocha, Nebraska Public Power District

Executive Summary

The NITC GIS Council recommends putting in place the Nebraska Statewide Imagery Program as a recurring program that facilitates the acquisition, historical preservation, maintenance, and distribution of high quality digital imagery and related products.

Imagery is the foundation of many of our Nebraska Spatial Data Infrastructure (NESDI) layers. The NESDI is a framework of geospatial data layers that have multiple applications and are used by a vast majority of stakeholders. These layers meet quality standards and have data stewards to maintain and improve the data on an ongoing basis. These layers are consistent with the Federal National Spatial Data Infrastructure (NSDI) and provide additional layers of particular importance to Nebraska.

The use of imagery has become a necessity and requirement for specific business functions through all levels of government and users in Nebraska. The business uses and needs of imagery vary by application. Each governmental entity (i.e., city, county, state) and political subdivision have varying requirements on timing and budgets. There are other components tied to acquired imagery that need to be considered such as, additional derived products, data hosting and map services. There is a need to develop a coordinated effort to support a recurring and sustainable imagery program for Nebraska. This program must also have flexibility to handle specific applications by its partners.

The imagery program will provide authoritative data that meets state imagery standards and will correspond with other NESDI layers. It will provide a level of visual registration and QA/QC in the derivation process of other NESDI layers. For example, it will provide parcel placement with respect to other land features and point addresses located at centroids of buildings. It will also be able to support future 3D visual representations when combined with LiDAR elevation data.

In general terms, a standard base product will include a minimum of a 30-cm (12-inch) pixel resolution "leaf-off" statewide orthoimagery product with ancillary data products and services. This is a recurring imagery program with orthoimagery collected every two or four years, depending on urban and rural area priorities. This will ensure that base orthoimagery would never be more than four years old for any part of the state. It will also allow partners to be included in an overarching contract and allow buy-ups of additional packages such as higher resolution imagery, oblique imagery, and planimetric layers such as building footprints. The program will also implement a preservation plan for the digital conversion and archiving of historical aerial imagery.

A statewide project has costs related to consistency, quality, completeness, maintenance of infrastructure for positional reference, data management, and public access to information. The minimum expected costs the initial year will be around $1.8 million. This includes the acquisition of a statewide orthoimagery product, data hosting and distribution, and program management.

Plans are to begin in early 2017 to identify funding sources and implement a procurement and vendor selection process that allows multiple levels of government, universities and other political subdivisions to purchase imagery and related products as soon as spring of 2018.

Budget shortfalls and goals to find cost savings provide the motivation to develop partnerships to reduce costs and explore all funding possibilities to ensure the success of the program. As more data is provided to the user community, the value of this data will gain further recognition. This will be accomplished by expanding existing data sharing and distribution methods to leverage historical and newly acquired imagery products so they are accessible. This program will also facilitate technical assistance and education outreach activities supporting the efficient utilization of imagery products. These activities will validate further support and funding to ensure the program has long term sustainability and success.

1.0 Program Justification

1.1 Program Needs

State and local governments, political subdivisions, and federal agencies working in Nebraska have demonstrated a need for accurate and precise aerial imagery data and services. Imagery products and services help them meet their varied business requirements for planning and management to support public services involving:

- property assessment
- public safety
- emergency management
- E9-1-1 / NG9-1-1
- utilities
- natural resources
- infrastructure
- transportation
- environment
- agriculture
- economic development
- planning
- recreation and public spaces

Why should Nebraska have an imagery program?

The answer to this question is based on a variety of factors that will be discussed throughout this business plan. These include the need for accuracy and uniformity in orthoimagery; timing and flexibility of imagery acquisition; reducing costs and duplication; preserving historical aerial imagery; and enhancing data distribution and consumption of imagery products.

Accuracy and Uniformity

There is a need for an authoritative orthoimagery data layer with survey and geodetic control that we can rely on for visual registration and compilation of data sets. The figure in Appendix I illustrates how imagery serves as a foundation for many other NESDI data layers. It provides the framework to conduct other map compilations and necessary visual registration processes to support data and mapping systems.

The level of required accuracy and uniformity of imagery products depends on the intended use of the data. Imagery is classified as either authoritative or referential (NSGIC, 2012). Authoritative imagery has specific mathematical and geometric properties necessary for creation of geospatial framework layers, while referential imagery refers to imagery having distortions from ground control.

The type of imagery required is dependent on its application and use. Appendix II illustrates examples of applications and identifiable features that can be measured at various spatial resolutions.

The context and intended application of current orthoimagery services do not meet existing needs and in many cases, standards. For example, the USDA Farm Services Agency (FSA) National Agriculture Imagery Program (NAIP) imagery is designed for assessment of governmental agriculture programs of crop, forestry, and other vegetation cover. Over the past 10 years, this product has been typically flown “leaf-on,” which does not allow for other necessary “leaf-off” applications. The pixel resolution for this product, typically 0.6 to 2 meters, as well as the horizontal accuracy, do not meet current Nebraska state standards. The acquisition schedule is currently on a two-year rotation and there is the uncertainty or risk of the continuation of the program.

The Nebraska Elevation Program plays an important role in the accuracy of imagery products. This program is established to acquire LiDAR data across Nebraska on an ongoing basis. Data such as LiDAR provide ground control and accurate elevation information that are used to process orthoimagery. Several LiDAR projects have been completed or will be finalized in 2018. This LiDAR data needs to be used in relation to imagery whenever it is available as long as it meets standards.

Using a set of uniform state imagery products for ongoing applications is critical, particularly when making comparisons in ground features across different locations. It also improves the proper classification of land use patterns derived from vegetative to bare soil conditions.

A recommendation of the Nebraska Statewide Imagery Program is the acquisition of orthoimagery for the entire state in a short 6-month time frame (i.e., fall to spring). This will avoid a “hit or miss” imagery acquisition on a piecemeal basis. Obtaining a standard orthoimage in a single time period is most beneficial as it provides a more uniform product, with similar color contrasts to ground features (i.e., drought versus wet year).

Once imagery has been acquired, it is important to implement proper quality control (QC) procedures that involve data users. Experiences gained from earlier projects have found that aerial images are time-sensitive and vendors need to deliver the products to the user to review as quickly as possible, even before they complete their own QC analysis. This way, the users get to see and use the imagery in a timely manner and also gain an opportunity to address potential imperfections prior to final delivery of the product. This type of workflow assumes that the imagery has already met a horizontal accuracy standard. There is a need to have a QC process where there are as many users evaluating it as possible.

Timing and Flexibility

A program that continues with ongoing re-flights is needed to capture feature changes on the earth’s surface (i.e., new developments, roads). Having a program that rotated every two to four years depending on the needs and applications would be ideal.

Timing of imagery acquisition must be considered in relation to vegetation condition. It is important to consider whether vegetative cover or no vegetative cover best meets a user’s needs. Imagery acquired “leaf-on” provides data for numerous agricultural and natural resource applications. Imagery that is flown in “leaf-off” conditions provides a clear view of ground conditions underneath tree canopies and other defoliated vegetation. This type of imagery is especially important for urban applications, such as property assessment and registering road centerlines and address points where heavy tree cover may obscure these features. The best time for flight acquisitions for leaf-off conditions are typically between mid-February to late-April. Re-flights may also be needed to account for feature changes on the earth’s surface (i.e., new developments, roads).

Not all geographic locations use the same orthoimagery deliverable products. Different areas of the state may have varying needs, depending on topography, population, and application requirements. There is a need for a program that would provide flexibility beyond a single baseline orthoimagery product. The program would need to provide opportunities for the buy-up of oblique imagery, higher resolution orthoimagery, and other specialized data such as thermal and infrared spectral imagery.

Reducing Costs and Duplication

Every effort should be taken to reduce duplication of imagery product acquisition and services. For example, if a city plans to fly a large portion of its area in a county, it may want to involve other nearby counties and cities. Putting aircraft in the air and planning flights over larger areas can cost about the same as flying to and from several small land areas within a region. Since certain costs are generally fixed, the overall costs can be reduced through using the economies of scale of the larger project.

There is also a need to reduce government staff time and multiple procurement procedures for duplicate acquisitions. Having a coordinated procurement process will promote cost savings and improve program auditing and evaluation.

Once data has been acquired for a joint effort, additional cost benefits can be gained in data hosting and shared technology applications. A data analysis application developed by one organization can be easily shared by other users using the same data. Web applications, once developed, can be used by multiple entities, thus leveraging costs even more.

Preserving Historical Aerial Imagery

Historical aerial imagery is a valuable resource, offering insight into the past, allowing us to know what existed in certain locations at a given time. Once it is digitized and georeferenced, it can be compared to other NESDI framework data and show changes that have taken place over time. For example, it can provide a context to historical surveys and deeds and the placement of boundaries. Many of the map surveys completed in the early 1900s referenced aerial photographs where boundaries followed old stream channels that no longer exist or have meandered over time. Other benefits of historical aerial imagery include the ability to monitor changes in natural habitats and understand environmental conditions caused by human activity. Some examples include, old contaminated sites such as buried landfills and man-made wetlands.

Enhancing Data Distribution and Consumption of Imagery Products

There is a need to leverage existing and new imagery products for a variety of applications. Imagery data files are large in size and it is not cost effective to host it in multiple locations. There is a need to enhance current methods that inventory, catalogue, and distribute large data sets. The state's Geospatial/GIS Enterprise system and NebraskaMAP have been established to begin this process. They provide a centralized repository for distributing data by several methods, including image tile downloads (i.e., clip/zip/ship) and web map services that allow users to consume imagery into their desktop mapping programs and online map viewers. There is a need for application programming interfaces (API) or plug-ins that can easily be incorporated into other applications. These add additional functionality in not just displaying data but also working with the data, such as making measurements or enabling other geoprocessing analyses. Along with the various ways to connect to and consume data products, there is a need for technical assistance and education to support the adoption of these technologies.

1.2 Strategic Foundation for a Business Plan

One of the four goals of the 2012 Nebraska Geospatial Strategic Plan is to facilitate the creation, maintenance, analysis, and publication of quality geospatial data. Imagery is classified as part of the NESDI and is defined as data that is obtained through aerial, satellite, and other sensor platforms to capture features about the surface of the earth. The NITC GIS Council has directed that a business plan for the acquisition, maintenance, and distribution of these imagery layers be developed. Furthermore, the NITC formally identified the NESDI as a new statewide strategic initiative in 2013 and identified the Nebraska Statewide Imagery Program as an action item to support the Governor's Statewide Technology plan.

Initial work has been the development and adoption of imagery standards by the NITC GIS Council (NITC 3-204 Imagery Standard, October 28, 2014). These involve data content standards, data schema descriptions, data compilation and accuracy standards, and metadata standards. A formal process will also be defined for the exchange of data and information between data stewards and the geospatial community of users.

There are other catalysts that have prompted the need for a statewide imagery program. These include coordinated efforts to improve and sustain an ongoing orthoimagery acquisition effort to meet federal and state requirements for property assessment, transportation, address point placement, and boundary

improvement projects. The state currently does not have a seamless statewide orthoimage that meets state standards. It will be necessary to collect a statewide orthoimage product in order to derive many of the essential NESDI data layers, including those that support current and future public safety and emergency services (i.e., enhanced/NG9-1-1) and various U.S. Census 2020 projects.

2.0 Goals and Objectives

2.1 Goal

The goal of the Nebraska Statewide Imagery Program is to produce a sustainable statewide imagery program for the state that facilitates the acquisition, historical preservation, maintenance, and distribution of high quality digital imagery products to be utilized for various governmental uses and for public consumption.

2.2 Objectives

The following objectives are essential to the success of the program.

1.0 Establish a program management team and operations plan with administrative coordination from the Geographic Information Office within the Office of the Chief Information Officer.

2.0 Establish and maintain standards, policies and strategies to emphasize cooperation and coordination among state, federal, county, municipality, utilities, university and other political subdivisions and organizations.

3.0 Identify and develop funding sources for program implementation and long term sustainability.

4.0 Implement a procurement and vendor selection process that allows multiple levels of government, university and other political subdivisions to purchase imagery and related products.

5.0 Develop and implement a preservation plan for the digital conversion and archiving of historical aerial imagery.

6.0 Expand existing data sharing and distribution methods to leverage historical and newly acquired imagery products so they are accessible, both publicly and for secure uses.

7.0 Provide communications, technical assistance and education outreach activities supporting the efficient utilization of imagery products.

8.0 Develop and implement an acquisition plan for statewide orthoimagery coverage and other products targeted for data collection beginning the spring of 2018.

9.0 Conduct a biennial evaluation and make necessary programmatic adjustments to procurement, standards, and other processes that impact activities and outcomes of the program.

3.0 Benefits

3.1 Anticipated Benefits

Orthoimagery products are easily recognized and can provide a useful framework layer for a variety of applications. Because many land features can be seen on an orthoimage, it can serve as a backdrop for visual reference, saving the expense of creating additional reference files. Orthoimagery helps users answer questions about identities, locations, distances, connections, proximities, surface waters, and structures. Timely emergency response, accurate and fair property tax assessment, more effective land use planning by local governments, efficient soil and water management, and timely delivery of products are examples of public and private benefits of regular, high resolution orthoimagery.

The Imagery for the Nation (IFTN) Cost Benefit Analysis describes non-quantifiable benefits of an orthoimagery program (USDA/USGS, 2007). Benefits may be organized into three categories: end-user value, governmental operational value, and private industry value.

Many benefits of an orthoimagery program to end-users are not quantifiable but are valuable in efficient and effective mapping, analysis, planning and decision support. End-user value may be expressed as:

- Access to current and historical imagery in the public domain, including access and distribution through NebraskaMAP
- Reliability of product and schedule
- Continuity of process and funding
- Opportunities to meet additional business requirements with buy-up options such as oblique imagery, increased resolution, or extracted map features
- Increased interoperability across jurisdictions through consistent datasets and cross-jurisdictional applications
- Common source data and metadata
- Higher resolution imagery for local users than previously available
- Access to consistent historical products to better understand landscape changes over time
- More applications available for decision support
- Increased user base through easier discovery of and access to imagery products

An orthoimagery program benefits governmental operations at all levels of government. These sources of value may be described as:

- Quality and consistency in operating data within and across jurisdictions
- Reliability of product and schedule to support planning, budgeting and analysis
- Standardization of procurement processes
- Application of standard data specifications and best practices
- Creation of economies of scale through consolidation of planning, budgeting, contracting and project management
- Interagency interoperability and consolidation of data storage and distribution
- Increased government user base through direct applications and service provider solutions
- More effective use of resources for other projects and programs that may include framework datasets such as elevation, thematic datasets such as building outlines, and analysis such as current land use.
- Coordinated and pre-planning of imagery acquisition helps budget and local planning expectations and timelines
- Improved government efficiencies through streamlined contracts and structured Request For Proposals (RFP) to guide contracting and auditing of acquisition programs

- Technical assistance and framework data modernization efforts that are also in sync with other NESDI efforts.

In emergency response by local government operations, benefits may be described as:

- Emergency responders can quickly assess how to get to the incident
- Emergency response has a better understanding of what may be required when they arrive
- Emergency response is better prepared in case assistance is needed outside of their region
- Time savings in call answering and response from better quality orthoimagery available to call centers (quality = consistency, currency, detail)
- Reduced confusion from multiple imagery datasets (e.g., reliance on a statewide "common operating picture")
- Improved existing GIS data framework layers to support enhanced and next generation 911

There are public examples of benefits stemming from improved government operations, some of which include:

- Imagery that informs accurate and fair assessment of local property taxes based on property boundaries and structures
- Natural hazard mitigation tasks that rely on imagery of prior conditions to better define ways to limit damage
- Understanding locations of specific public service needs
- Orientation and documentation of land, buildings, transportation and other features important to economic developers
- Geospatial information dissemination
    - Road Centerline gathering
    - Structure collection
    - Parcel information gathering
    - Time savings in local tax offices, GIS operations and related local operations
- Improved taxpayer satisfaction through partnership efforts that reduce costs on collective imagery

An orthoimagery program benefits the geospatial data industry and other private businesses. Service providers include contractors or subcontractors for aerial image acquisition, image processing, quality control, maintenance of base mapping layers, creation and maintenance of thematic layers, custom mapping, and mapping applications.

Orthoimagery producers in Nebraska have included large firms that are national in scope, medium firms with regional scope, and small firms that work primarily within the state. There are many small firms in Nebraska that benefit from a market dominated by frequent locally-funded imagery projects.

Private industry value may include:

- Increased opportunity for value-added services such as feature extraction, base mapping, and processing of color infrared imagery
- Guidance for coordinating efforts across counties and in service to state agencies
- Common source data for applications across the state
- Improved planning and scheduling of workflow for professional service providers
- Positive economic impact
- Increased customer base

Many more private and nonprofit organizations derive benefits from current, high resolution imagery in applications related to real estate, product delivery, engineering, planning, environmental assessment, and a variety of other uses.

The Nebraska-Iowa Regional Orthoimagery Consortium (NIROC) has indicated several qualitative benefits of a regional imagery acquisition program. The following are some examples from that program:

- More volume = more negotiating power = lower prices
- Pooled internal technical knowledge and experience
- Seamless imagery products across jurisdiction lines. This becomes useful for public safety and natural resource applications.
- Larger projects typically mean higher priority and response from the vendor
- The ability to spread payments over multiple fiscal years enables smaller and more rural communities to participate
- Improved collaboration, networking, and communication between various agencies

3.2 Return on Investment and Shared Value

The returns one would expect to find in the initial investment of imagery products and services are typically a measurement of cost savings and shared value among users.

Since Nebraska has not obtained a statewide orthoimagery product, there is no exact data to predict a return on investment. However, you can determine from other state programs, who have been conducting their program for many years, that statewide imagery programs prove themselves valuable and benefit taxpayers.

Based on the findings from other states, adopting a state-wide imagery program has been cost effective.

- Indiana reports a 34:1 return on investment over a three-year period for an initial investment of $7,432,625 that included data acquisition and distribution.
- Florida has predicted that an ongoing annual investment of $2.9 million that supports statewide orthoimagery in their state that yield $31.1 million in annual benefits. The greatest reported benefits were from a reported $1.96 million per year staff productivity and labor cost savings. The benefits from reduced costs through joint funding of orthoimagery projects were reported at $1.82 million per year. This clearly demonstrates that even if there is not a formal coordination effort in place, organizations are working together to maximize the benefits to their organizations.
- Maine has shown annual investment returns in their program of 421% to 1264%, based on net benefits ranging from $10 to $30 million. Their program further leverages their state funds at better than a 2.5 to 1 ratio.

The resources to support these state imagery programs were predominately supported through enhanced 911, emergency management, and other transportation funded projects.

Measuring and translating benefits to dollars is difficult and approximate, but useful in framing the value of statewide orthoimagery. The following descriptors of benefits can be translated to return on investment: a) time / efficiency for informing public decisions, b) currency of imagery and features (cost of misinformation), and c) time for handling, storing, retrieving, displaying, and archiving imagery data. These descriptors for return on investment will be documented through the life of the program ensuring ongoing investments match the need and benefits of the program.

4.0 Background

4.1 Remote Sensing 101 and the Context of Products in this Business Plan

There are several different remote sensing platforms that capture digital imagery. For example, aircraft (i.e., aerial), satellites, Unmanned Aerial Systems (UAS), and physical mounted platforms. The most commonly used platforms for the majority of governmental applications include data collections from aerial, satellite and UAS platforms.

The type of sensor and analysis techniques used with these platforms produce a digital data product. The most widely used products include: orthoimagery, oblique aerial imagery, and Light Detection and Ranging (LiDAR). Today, newer technologies use photon and geiger sensors. Combinations of these platforms and sensors allow for the depiction of physical structures on the earth's surface.

Orthoimagery

Orthoimagery data typically are high resolution aerial images that combine the visual attributes of an aerial photograph with the spatial accuracy and reliability of a 2-dimensional horizontal map. An orthoimage is a uniform-scale image where corrections have been made for feature displacement such as building tilt and for scale variations caused by terrain relief, sensor geometry, and camera tilt.

Oblique Imagery

Oblique imagery is what the name suggests. It is a technique of aerial photography that provides detail from a 45 degree angle with the ground. It more closely resembles how people normally view their landscape compared to traditional orthogonal (straight down) imagery. Many counties, municipalities, and projects are interested in oblique imagery as it provides additional details around buildings and tall structures. The data products for oblique imagery acquisition vary by vendor and application.

Historic Aerial Photography

Historical aerial images are derived from analog photography that is imaged onto film. These uncorrected images are not digitized. Once scanned, they go through an orthorectification and geo-referencing process to put them in a digital format that provides a level of accuracy for making measurements.

Historical aerial photos are an invaluable resource for farmers and land owners, consultants, and government agencies. Uses can include land use/land cover change detection, applications for environmental studies, community planning, historical records of boundaries and many others.

Other Remote Sensing Technologies

Other products can be provided through remote sensing instruments. There are two types of remote sensing instruments—passive and active. Both types are able to potentially detect traits of objects that may not be visible to the human eye, such as infra-red, thermal, multispectral and hyperspectral characteristics. Both passive and active sensors can be deployed from a variety of platforms that include satellites, airplanes and UAS.

Passive instruments detect natural energy that is reflected or emitted from the observed scene. They sense only radiation emitted by the object being viewed or reflected by the object from a source other than the instrument. Sunlight is the most common external source of radiation sensed by passive instruments. Examples include cameras and specialized devices such as radiometers and spectrometers, which measure electromagnetic radiation using a variety of detectors.

Active instruments provide their own energy (electromagnetic radiation) to illuminate the object or scene they observe. They send a pulse of energy from the sensor to the object and then receive the radiation that is reflected or backscattered from that object. Examples of active sensors include radar and LiDAR.

4.2 History of Nebraska's Imagery

Historically, the consumption and usage of digital imagery across Nebraska has relied mostly on the federal programs and local projects across the state. Aerial photographs were collected as far back as the late 1800s using black and white print film. Since 1993, it is estimated that more than $14.2 million has been spent on some level of aerial acquisition in our state. The following is a brief summary of those acquisition projects.

US Geological Survey (USGS)

Nebraska's first statewide orthoimagery was the delivery of US Geological Survey (USGS) digital orthophoto quarter-quads (DOQQs) in 1993 and 1999. This was a partnership between the NDNR and USGS. This effort implemented the National Mapping Standards for primary digital ortho-photoquadrangle (DOQ) requiring a 1-meter ground resolution for quarter-quadrangle (3.75-minutes of latitude by 3.75-minutes of longitude) image. It was casted on the Universal Transverse Mercator Projection (UTM) on the North American Datum of 1983 (NAD83) and mapped to 1:12,000 scale. The vertical accuracy of the verified USGS format DEM is equivalent to or better than a USGS level 2 DEM. There is no record on the total cost for these two years of imagery.

USDA FSA National Agriculture Imagery Program (NAIP)

The primary goal of the NAIP program is to maintain common land unit (CLU) boundaries and assist with farm programs (i.e., estimation of crop and other vegetative cover). The NAIP imagery program has been predominately financed at the federal level with the opportunity for local "buy-ups" of higher resolution data. The NAIP imagery resolution collected for Nebraska is a 1-meter ground sample distance (GSD) for 2003, 2006, 2007, 2009, 2010, 2012, and 2014. In 2004 and 2005, imagery was collected for compliance uses at the resolution of a 2-meter GSD. As technology and sensors continued to improve, the cost effectiveness also improved, so the 2016 imagery was acquired at 0.6-meter. The spectral resolution is provided in 4-bands, containing red, green, blue, and near-infrared bands. NAIP quarter quads are formatted to the UTM coordinate system using NAD83. Total estimated cost spent on this imagery through USDA to date is $8,751,364.20 for Nebraska.

University of Nebraska

Since 1986, the Center for Advanced Land Management Technologies (CALMIT) at the University of Nebraska-Lincoln has been acquiring remotely sensed satellite (primarily Landsat and MODIS) imagery. CALMIT's mission is to enhance and expand research and instructional activities in remote sensing, geographic information systems (GIS), automated cartography and image processing. Until much of the imagery became available for free in 2008, acquisitions by CALMIT were made on an as-needed basis and purchased using research grant funds. Nebraska Landsat images related to research projects are available to the public via the NebraskaView website (http://nebraskaview.unl.edu/), although that data is now also readily available through various federal data gateways.

Over its history, CALMIT has also been involved in a number of landuse mapping activities in conjunction with various Nebraska state agencies. The 2005 Nebraska Land Use map was developed through funding by the NDNR, while irrigation maps from the late 1990s through the mid-2000s were developed under the auspices of the Platte River Cooperative Hydrology Study, a multi-agency effort with the objective of improving the understanding of the hydrological conditions in the Platte River watershed in Nebraska upstream of Columbus, Nebraska.

The School of Natural Resources, University of Nebraska at Lincoln (UNL), houses the largest public archive of historical Nebraska aerial photos in the state. The 9" x 9" black and white photos are at a scale of approximately 1:20,000 and were obtained through UNL's Conservation and Survey Division (CSD) from the U.S. Department of Agriculture's (USDA) Farm Service Agency (FSA). The archive is cataloged by county for each year available. Although complete statewide coverage is not available, the archive includes photos from the 1930s to the 1970s and generally includes one set of photos for each decade.

Nebraska-Iowa Regional Orthoimagery Consortium (NIROC)

The Nebraska-Iowa Regional Orthoimagery Consortium (NIROC) consists of cities, counties, natural resource districts, and state and federal agencies in the eastern most part of Nebraska. It has involved the core Nebraska and Iowa urbanized areas but has also been open to other entities to participate. The project is currently on a three year acquisition cycle that started in 2007 and most recently collected data in 2016. The latest acquisition included collection of 3, 4 and 6 inch orthoimagery and obliques. Total investment to date for imagery acquisition is $5.3 million.

Central Nebraska Consortium

The Central Nebraska Consortium involves eight cities and two counties. It collected data in 2007 with 6 and 12 inch imagery.

4.3 Imagery for the Nation

Imagery for the Nation (IFTN) is a National States Geographic Information Council (NSGIC) led effort to encourage the federal government to fund consistent, regular orthoimagery acquisitions across the U.S. (http://www.nsgic.org/imagery-for-the-nation). NSGIC is currently examining options to work with all states to pursue improved contracting mechanisms to further reduce costs on orthoimagery products.

Recent discussions have involved working with federal government partners such as the USDA FSA NAIP program. Thus far, no funding has been appropriated by USDA or other federal government agencies for this effort.

As sensor technology improves over time, it may become more affordable and timely to handle high-quality imagery acquisition for state needs at a regional rather than federal level.

5.0 Program Requirements

The NITC GIS Council recommends establishing a recurring program that can periodically re-fly the state to make high quality imagery and related products available statewide. Several requirements to achieve the goal of this program are addressed in this business plan. These are summarized in the following components:

Program Requirement Components

- Organizational structure
- Legislative support
- Data, application and product components
- Standards
- Technology requirements
- Human resource requirements
- Costs
- Finance and Procurement Strategy
- Reduction of Risk

5.1 Organizational Structure

The NITC GIS Council and the Imagery Working Group are responsible for the development and recommendations found in this business plan. These individuals are identified in the acknowledgement section of this business plan. The following groups have a role in the governance and responsibilities for planning and implementation of a statewide imagery program.

NITC GIS Council

The NITC Geographic Information Systems Council was established by the Legislature in 1991 (Reissued Revised Statutes of Nebraska, 1943, §86-569 through §86-573). The Council serves as the state's primary oversight group for the development of standards, strategies, and policies as they relate to the creation and use of geospatial data and technologies. The Council emphasizes cooperation and coordination among agencies, organizations, and government entities. These coordinated efforts lead to creating public and private partnerships, greater geospatial productivity, less redundancy, and more informed policy across all disciplines and business lines involving geospatial data and technologies in the state. The GIS Council mission is to:

> *"Encourage the appropriate utilization of GIS technology and to assist organizations to make public investments in GIS technology and geospatial data in an effective, efficient, and coordinated manner."*

This council is made up of twenty six representatives appointed by the Governor representing diverse stakeholders. The stakeholders are representatives from state, county, municipal and federal government agencies, and other public and private entities using GIS/geospatial technologies as they relate to the geographic area of the State of Nebraska. The main purpose of this body is to represent the needs and ideas of the broad statewide NESDI community and to serve in an advisory role to the NITC, the Office of the CIO, and legislative body.

Imagery Working Group

The GIS Council implemented an Imagery Working Group in 2012 (NITC GIS Council, 2016). This Working Group takes the lead in identifying issues, soliciting input, and recommending solutions for imagery products and services paid by taxpayers. As part of this process, the working group pursues input and feedback on all aspects of the program geospatial imagery from partners not directly participating on the working group.

The Working Group was directed to develop a business case outlining the need for a statewide imagery program. The Working Group has submitted this business plan as a recommendation to the NITC GIS Council. The Council may accept, modify, or reject those recommendations. It is more than likely that members of the Imagery Working Group will transition into the Nebraska Statewide Imagery Program Management Team.

Nebraska Information Technology Commission

The Nebraska Information Technology Commission (NITC) is a nine-member commission established by the Legislature (Neb. Rev. Stat. § 86-515 to 86-86-518) to provide advice, strategic direction, and accountability on information technology investments in the state. To achieve its mandate, the NITC relies on coordination and collaboration to influence a wide range of information technology issues. The NITC annually prepares a Statewide Technology Plan, provides biannual recommendations on technology investments to the Governor and the Legislature, and adopts technical standards, guidelines, and architectures. The NITC is assisted by six advisory groups: the Community, Education, eHealth, GIS, and State Government Councils and the Technical Panel. Standards and guidelines recommended by the GIS Council are sent to the Technical Panel for 30 day review prior to submission to NITC for review and approval.

Office of the Chief Information Officer

The Office of the CIO (OCIO) (Neb. Rev. Stat. § 86-519) is located within the Department of Administrative Services which provides administrative and budgetary services for the office. The OCIO provides overall IT policy, governance, planning and oversight, IT coordination for state agencies, and development, oversight, and operation of enterprise shared systems. It provides administrative oversight to the Geographic Information Office and the NITC GIS Council. The Chief Information Officer is a designated member seat on the GIS Council.

Geographic Information Office

The Geographic Information Office resides in the OCIO and serves as the state's governmental operations and management body for GIS and the NESDI. The office is led by the State GIS Coordinator. Staff is currently being expanded through consolidation efforts to respond to increased requirements for the NESDI coordination and operational support and administration of the Geospatial/GIS Enterprise platform. This group provides the necessary coordination of funding and procurement activities to support the NESDI strategic initiative action items designated by the NITC. The State GIS Coordinator has authority to enter in statewide contracts and has support for administrative and budgetary services.

5.2 Legislative Support

The Nebraska Imagery Program is a strategic initiative identified by the NITC and the Governor's Statewide Technology Plan. According to Neb. Rev. Stat. § 86-572(2), committees, duties. The NITC GIS Council shall: *"(1) Make recommendations to the Legislature and the Nebraska Information Technology Commission for program initiatives and funding."*

The member representation on the NITC GIS Council includes the same partners involved in recommending a statewide imagery program. These partners represent several levels of government that have different responsibilities and governance when making decisions.

Nebraska's challenge is to coordinate several systematic statewide data layer acquisition efforts around various funding cycles and other constraints. This requires making plans for acquisition, procurement, stewardship, distribution, and coordinating future programs in a way that they also work together. These organizational needs would be more efficient and effective if addressed under a state program.

Legislation plays an important role when it comes to building cooperation among various political and governmental entities. It is important that the Nebraska Legislative body is aware of these efforts and the recommendations outlined by this business plan. It recommends legislation in support of a coordinated statewide effort that has many cost benefits to taxpayers.

Legislative support is needed in several ways. One is the overall awareness and recognized value of NESDI data layers such as imagery. Particularly, how they benefit the public and are used in various government applications to support public services.

The Legislative body can also make a difference by making sure that existing and newly introduced legislative bills support common themes of the business plan. These items can include:

- Recognizing that there is a coordinated effort through the NITC GIS Council, the Office of the CIO, and a Program Management Team to advise and manage operations of a statewide imagery program. These entities have expertise and efficiencies in acquiring, using, and distributing data.
- Ensuring that legislated programs are using taxpayer funds efficiently. This ensures that data and services are not being duplicated.
- Supporting funding for sustainable and timely acquisition and distribution of NESDI data for meeting specific program requirements at all levels of government. For example, future

coordinated GIS data expenditures to support public safety (i.e., enhanced/NG9-1-1), emergencies, and economic development.

5.3 Data, Application and Product Components

The following data, application and product components are organized by orthoimagery, obliques, historical imagery, and other remote sensing products. It includes consideration of data formats, hosting, and related map services and viewers to support the distribution and consumption of the data.

5.3.1 Statewide Orthoimagery

Produce an orthoimagery product with seamless coverage across the state and across navigable waterways to other state shorelines (i.e., Missouri River coverage) that has the following characteristics.

- Acquisition of orthoimages at a minimum 30-cm (12-inch) pixel resolution, delivered in 5,000 x 5,000 foot grid tiles.
  - Provide the option, if cost effective, for buy-up of 15-cm (6-inch) and 7.5-cm (3-inch) resolution imagery for specific counties, municipalities, or project areas with varying sizes of coverage areas.
- 4-band (RGB+IR) imagery
- Leaf-off (i.e., majority of deciduous and other vegetation have no leaves)
- Data acquisition occurs during fall to spring and meets specific ground and atmospheric conditions, and other specifications identified in state standards.
- After the first year of statewide imagery coverage, the frequency will continue at every 2 years for urban and prioritized areas and every 4 years for the entire state.
  - Rural counties can have the option to buy-up every two years, if needed. The determination of urban versus rural areas are dependent on local needs and when these acquisition periods should occur.
- The following formats and services to support this data.
  - Data hosting for raw tiles, inventoried electronically, and/or mosaic of imagery files
  - Option for formats and derived products such as Enhanced Compression Wavelet (ECW) and Mr. SID, 3D (end lap/side lap) capture, planimetric capture and other analysis for feature extraction, impervious surfaces, building footprints, land use / land cover, and other vegetative indices.
  - Web map services that deliver and support OGC Web Map Service (WMS)
  - Application viewers and API capabilities for data review, measurement tools, and integration with other web mapping applications and viewers.

Additional data, application and product specifications for orthoimagery are provided in more detail in the Imagery Standards (NITC 3-204, 2014).

5.3.2 Obliques

Produce low-level oblique images at four cardinal directions with the following characteristics.

- Acquisition of oblique imagery at a minimum 15-cm (6 inch) pixel resolution for urban areas and 30-cm (12-inch) for rural areas.
- 3-band (RGB) imagery
- Leaf-off (i.e., majority of deciduous and other vegetation have no leaves)

- The frequency of data collection depends on the intended application and the level of imagery needed for property assessment. Consideration for data frequency should be made to support the Standards for Mass Appraisal of Real Property. Whereas, obliques must be collected no less than every two years for urban areas and 6 to 10 years in slow growth areas.
- Data acquisition occurs during fall to spring and meets specific ground and atmospheric conditions, as wells as other related specifications similar to those found in the orthoimagery standards.
- The following formats and services to support this data.
    - Data hosting for original images that are cataloged/indexed and have metadata
    - Application viewers and API capabilities for data review, measurement tools, and integration with other web mapping applications and viewers.

5.3.3 Historical Aerial Imagery

Produce a digital library of historical aerial photographs from paper and film with the following characteristics.

- A comprehensive discovery and inventory process to identify the various historical photographs in paper and film and determine if they are of quality to be digitized.
- Preservation of historical imagery follows best practices and other standards for proper indexing, scanning and digitizing, geo-referencing, rectification, and attribution.
- The following formats and services to support this data.
    - Data hosting for raw tiles, inventoried electronically, and/or mosaic of imagery files
    - Web map services that deliver and support OGC Web Map Service (WMS)
    - Application viewers and API capabilities for data review, measurement tools, and integration with other web mapping applications and viewers.

5.3.4 Other Remote Sensing Products

There are other remote sensing technologies and value-added services for use with imagery-based products. Many of these products are specific to certain users and applications and are best handled as separate contracts due to their nature and timing. They deserve mention in this business plan as they are recommended for meeting specific business needs. The following are a few notable remote sensing products and deliverables that are commonly used in Nebraska.

- Aerial platforms that provide multi-spectral, hyperspectral, and thermal sensory wavelengths to support applications that need to go beyond the typical color and infrared bands.
- Light Detection and Ranging (LiDAR) that provides highly accurate digital elevation data. This data comes in the form of point clouds indicating heights of objects above the ground surface.
    - A separate NESDI business plan was completed in 2014 for a Statewide Elevation Program. There are state standards for supporting the acquisition of LiDAR for elevation in Nebraska (NITC 3-203, 2014).
- Satellite provides a different resolution and scale of orthoimagery and obliques including other sensory bands and wavelengths (i.e., RGB, IR, multispectral, thermal). This information has been used in the past due to the quick turnaround of imagery for remediation response to emergencies and natural hazards such as tornados, grass/forest fires, and flooding.
- Unmanned Aerial Systems (UAS) are designed for low-level and small-scale projects and can be equipped with various sensors to support many uses and applications. There are federal laws and policies in place through the Federal Aviation Administration (FAA) that limit the operation of UAS under certain areas and circumstances.
- There are other derived products from imagery using software and computational methods either as standalone products or for use in combination with other imagery products. These can include planimetric capture and other analyses for feature extraction; change detection;

classification procedures for determination of impervious surfaces and land use / land cover; vegetative or bare soil indices; stereo imagery; and 3-D data/models.

5.3.5 Data Distribution and Sharing of Data

All data obtained through this effort would be made public and are subject to the Nebraska Public Records Law. There is no foreseen requirement for data sharing agreements other than where specific licensing and service agreements are in place at the time of procurement or usage during events initiated by declared states of emergencies and national/homeland security. This includes data that is restricted by licensing or privacy restrictions and only shared on a limited basis according to terms specified in the license.

The data will also be made available through multiple formats (i.e., raw tiles, web map services). This will further leverage imagery for use in core function areas and business functions that inventory and reference ground based features, analyze and model relationships with other data, and provide basic visualization processes.

All data deliverables will be made available through the NebraskaMAP geospatial data clearinghouse by the program stakeholders. NebraskaMAP provides a centralized enterprise-level data-sharing platform intended for users needing access to geospatial data in the state. A NebraskaMAP Data and Content Management Policy was established to outline processes to share data and define responsibilities among data stewards (NebraskaMAP, 2016).

5.4 Standards

5.4.1 Nebraska Imagery Standards

Initial work has been completed to develop required specifications for orthoimagery acquisition to be used through the statewide imagery program. These specifications went into the development of standards and have been approved for orthoimagery acquisition for Nebraska. These were approved October 28, 2014 by the NITC (NITC 3-204, 2014). These standards will be updated to reflect the American Society for Photogrammetry and Remote Sensing (ASPRS) standards that were finalized November of 2014.

Data acquisition of imagery products are expensive and require preplanning. This standard provides requirements necessary for the creation, development, delivery, and maintenance of aerial imagery acquisition to support a statewide Nebraska Imagery Program. Since there are multiple uses for imagery, these standards are set at a minimum such that the majority of applications and needs are met across the state. These standards do not take into consideration other imagery products such as obliques and satellite products.

5.4.2 Other Referenced Standards

Other standards and guidelines were used in the development of Nebraska's state standards. These include ASPRS, NENA, and Mass Appraisal guidelines.

<u>American Society for Photogrammetry and Remote Sensing (ASPRS)</u>

The ASPRS Positional Accuracy Standards for Digital Geospatial Data were finalized in November of 2014. (ASPRS, 2014). These standards outline positional accuracy standards based on RMSE thresholds for digital orthoimagery.

1. Accuracy Requirements for Aerial Triangulation:

$$RMSE_{x(AT)} \text{ or } RMSE_{y(AT)} = \tfrac{1}{2} * RMSE_{x(orthoimagery)} \text{ or } RMSE_{y(orthoimagery)}$$

$RMSE_{z(AT)} = RMSE_{x(orthoimagery)}$ or $RMSE_{y(orthoimagery)}$

2. Accuracy Requirements for Ground Control Used for Aerial Triangulation:

$RMSE_x$ or $RMSE_y = 1/4 * RMSE_{x(orthoimagery)}$ or $RMSE_{y(orthoimagery)}$,

$RMSE_z = 1/2 * RMSE_{x(orthoimagery)}$ or $RMSE_{y(orthoimagery)}$

3. Accuracy Requirements for Orthoimagery:

Orthoimagery for this program should be produced to meet the following horizontal accuracy figures:

Orthoimagery Pixel Size (cm)	**Horizontal Accuracy Class**	**Absolute Accuracy**			**Orthoimagery Mosaic Seamline Mismatch (cm)**
		$RMSE_x$ and $RMSE_y$ (cm)	**$RMSE_r$ (cm)**	**Horizontal Accuracy at 95% Confidence Level (cm)**	
	X-cm	≤*X*	≤1.4142* *X*	≤2.4477**X*	≤ 2**X*
7.5	*11.25*-cm	≤*11.25*	≤15.90	≤27.53	≤ 22.5
15.0	*22.5*-cm	≤*22.5*	≤31.82	≤55.07	≤ 45.0
30.0	*45*-cm	≤*45*	≤63.64	≤110.15	≤ 90.0

National Emergency Number Association (NENA)

The use of imagery products for deriving other map coverages are outlined in the NENA GIS Data Collection and Maintenance Standards (NENA, 2007). These standards outline the minimum requirements of using orthoimagery for use in compiling source maps. Digital orthoimagery or raster data shall have a scale of 1:2400 or better with a minimum 12 inch pixel resolution which produces a NSSDA Horizontal RMSE (Root Mean Squared Error) Accuracy level of five feet or better. These standards are in the process of being modified for next generation 911 purposes and will potentially either increase in accuracy requirements or stay the same.

International Association of Assessing Officers (IAAO)

The IAAO has produced a standard on Mass Appraisal of Real Property (IAAO, 2013). The objective of the standard is to provide a systematic means by which concerned assessing officers can improve and standardize the operation of their offices. These standards are advisory in nature and the use of, or compliance with, such standards are purely voluntary. The defined digital imagery is acceptable for use in property assessment. These data products include high-resolution street-view images and data obtained from aerial platforms such as orthoimagery, low-level oblique images, and LiDAR.

The standard states that orthoimagery must have a minimum 6 inch pixel resolution in urban and 12 inch in rural areas. Low level oblique images capable of measuring for verification purposes, should be collected in four cardinal directions, with a minimum pixel resolution of 6 inches in urban and 12 inch in rural areas. The frequency for orthoimagery and obliques should be collected within a minimum of every 2 years for rapid growth areas, and 6 to 10 years in slow

growth areas. The standard suggests that either one of these products can be obtained in those time frames, since it is used for verification purposes.

Nebraska Information Technology Commission (NITC)

Other references are made to imagery standards through the following NITC standards.

- *NITC 3-201 Geospatial Metadata Standard*
  State agencies and other applicable state funded entities shall complete ISO 19115-compliant metadata documentation of existing and applicable geospatial data holdings.

- *NITC 3-205 Street Centerline Standard*
  Capture scale for digitizing is 1:2400. Street centerline placement can be completed using aerial imagery that meets verified horizontal accuracy requirements for spatial resolution (12 inch minimum), preferably leaf-off.

- *NITC 3-206 Address Standard*
  Capture scale for digitizing is 1:2400. Address point placement can be completed by visual registration using aerial imagery, site plans or other graphical resources that have been spatially adjusted to meet minimum spatial accuracy requirements. Using aerial imagery that meets verified horizontal accuracy requirements for spatial resolution (12 inch minimum), preferably leaf-off.

5.5 Technology Requirements

The necessary technology requirements to fulfill this program will consist of internal and external resources. The acquisition, quality control, and specific deliverables of imagery products are best handled from external industry partners. There are many qualified photogrammetric, engineering, and surveying firms who are experienced with this technology, and are interested in competing for the State's business. The state Imagery Standards will serve as the necessary specifications for obtaining orthoimagery products. Other imagery products to be acquired will still need to be scoped out for meeting specific needs and timelines.

State government agencies have begun enhancing their technology infrastructure the past two years to support the distribution and leveraging of large data sets such as imagery and other remotely sensed products. The OCIO Geographic Information Office is leading this effort with the Geospatial/GIS Enterprise solution as part of state government's IT Consolidation Plan. It is currently finalizing the migration of several state agencies into a shared data and map services platform.

This platform provides a secure file server and database infrastructure that reduces duplication of data, promotes data sharing, and further builds efficiencies when leveraging geospatial data to support business functions. This infrastructure builds support from external software and service companies. Additional efforts are underway to further reduce data storage costs by utilizing other cloud based solutions.

The Conservation and Survey Division at UNL currently supports the necessary technology requirements for the preservation of historical aerial photographs. They plan to continue the historical preservation of aerial photographs for the state as resources permit. They are in the process of scanning and geo-referencing approximately 250,000 aerial photos. Support for this effort comes from grant funds provided by the USDA Natural Resources Conservation Service.

The statewide orthoimagery product and other deliverables used by state agencies will be hosted with the enterprise platform and extended through NebraskaMAP. The clearinghouse provides both public and secure access to authoritative geospatial data commonly used across the state. It provides a mechanism to "roll-up" data to a statewide framework to support many regional and statewide business functions.

Imagery metadata and indexing of pertinent data files will make it easier for partners and data users to search and find data. The clearinghouse is also propagated with ISO taxonomy and keywords that meet federal standards so that it can easily be rolled up into federal clearinghouses such as GISInventory.net and data.gov.

Partners who participate with the statewide imagery acquisition portion of the program can participate with these solutions. Certain applications and web map viewers may have license or usage restrictions to certain data types such as oblique imagery. The procurement plan will provide other options to host data and provide map services to support these types of imagery products.

As technology and interoperability of data between mapping systems improve, it is possible there will be ways to reduce duplication of data hosting and other cost efficiencies.

5.6 Human Resource Requirements

5.6.1 Program Coordination

From a statewide program management level, the program will rely on the existing infrastructure to implement this plan by relying on existing lines of communication and processes. The State GIS Coordinator oversees current statewide contracts and can initiate and implement into agreements that support state government and other political subdivisions. The OCIO Procurement Team and Department of Administrative Services will provide support for the procurement, award selection, and billing for product and services rendered under this program. A representative of the OCIO Project Management Office will also be assigned to keep program objectives on time. A percentage of time from the program manager, procurement, and project management support staff will be dedicated to provide sufficient oversight and coordination for the Nebraska Imagery Program.

5.6.2 Program Management Team

A Program Management Team will be formed in an advisory capacity to assist in the development and maintenance of the operations plan, request for proposal (RFP) and communicate the business plan objectives to stakeholders. The program management team will be led by the State GIS Coordinator within the OCIO Geographic Information Office and will consist of representatives in state, county, city, University and federal government.

A similar recommendation for a program management team has been made as a result of the Nebraska Elevation Program. There are similar roles and partners involved in that program management team. This business plan recommends to evolve these two program management teams into one group, covering both imagery and elevation efforts in the state since much of the procurement processes are the same.

5.6.3 Other Expertise and Support

At the local level, many counties that participate in the procurement and delivery of imagery products have staff to develop scopes of work, contract negotiation and management, quality assurance/quality control and even distribute and work with the data. The primary changes from their process will be management of funding and working with state level procurement contracts for acquisition and delivery of imagery products and services.

Cities and counties that have their own GIS staff will continue to leverage the imagery products to support their current business operations. They will also participate in evaluating imagery products prior to delivery.

There currently exists information technology support staff at the state government level through the OCIO and other supporting state agencies to accept the delivery of imagery products and leverage them into state business operations. This support relies on current industry contracts for software and services to deliver and analyze imagery products.

- The OCIO staff will oversee the data hosting, map services, and distribution of data and deliverables within the Geospatial/GIS Enterprise platform. They will leverage data holdings current map applications and NebraskaMAP.

- The Department of Roads has expertise in photogrammetry and has experienced staff who are efficient in using photogrammetric software. They are responsible for incorporating imagery products and ground control in to their workflows to produce map designs for planning and litigation for roadway projects.

Additional expertise from the Conservation Survey Division at UNL and research community will be available in preserving historical imagery and developing geoprocessing tools to support imagery products. There is a need to expand expertise among the research community in developing and proving geoprocessing tools in this area. These tools require research and would improve confidence levels over time so they could be implemented within local and state government business operations. Some examples include: developing models for change detection that support various geometric features from vegetation to structures, assisting in improving data quality and other analysis techniques with various remote sensing data sources.

5.7 Costs

A request for information (RFI) was initiated in late 2015 to acquire specific cost estimates for the acquisition and delivery of various imagery products. There were five photogrammetry companies that provided information to the request.

Orthoimagery

For orthoimagery acquisition, minimum and maximum cost estimates were obtained by specific sized coverage areas in square miles (Table 1). Orthoimagery estimates are based on products meeting the imagery standards. Acquisition services vary depending on how they handle costs for quality control and delivery of the final product.

Table 1. Estimated minimum to maximum costs for orthoimagery acquisition by size of coverage area measured in square miles.

	Minimum – Maximum Costs *$ / square mile*		
Coverage Area *square miles*	**12 inch***	**6 inch**	**3 inch**
30,000+	$22 - $52	$55 - $109	$175 - $275
10,000-30,000	$55 - $109	$60 - $110	$179 - $300
400-10,000	$43 - $125	$66 - $250	$196 - $450

*One vendor produces a 9 inch product rather than 12 inch at $75 for all coverage sizes.

Cost data presented here suggests economies of scale (i.e., large areas acquired reduce costs per unit of orthoimagery delivery). The total estimated costs for statewide coverage for a 12 inch resolution product would be approximately $1,780,000. This is assuming an average price of $23.00 per square mile.

Many states have statewide initiated imagery programs. Other states have acquired a minimum 12 inch resolution orthoimagery product similar to our state standards. During the past seven years they have reported costs between $40 to $104 per square mile. This averages to $72 per square mile. The costs

differ depending on how the product is acquired and delivered (e.g., buy-up features and other processing costs). Table 2 shows some example states data acquisition costs by product type and year.

Table 2. Other state examples of orthoimagery acquisition costs by year.

State	Year	Description	Cost Per Square Mile
Florida	2012	$2.86 million/year investment benefits back $32 million/year	$95
Kansas	2014	12 inch, leaf-off, RGB+IR	$22
Indiana	2013	$4.7 million one time for 4-band. Map entire state over a 3 year period.	$126
Michigan	2016	base 4-band, additional costs for buy-ups.	$28
North Carolina	2010	6 inch, RGB	$250

It is also important to note that image acquisition has dropped in price over the past several years largely due to improved efficiencies in the technology.

The expense to acquire and process imagery is exponential in costs as you acquire higher resolution information (e.g., 1 foot going to 6 inch) to depict out ground features.

Oblique Imagery

Oblique imagery products come in various resolutions ranging from 1 inch to 12 inch. Some of the most common resolutions used by municipalities are between 2 and 9 inch resolutions. Costs for oblique imagery obtained in the RFI are summarized in Table 3.

Table 3. Estimated average minimum to maximum costs for 4-way oblique imagery acquisition by resolution.

Resolution	Estimated Costs, $/sq. mile
9 inch	$140 - $205
6 inch	$197 – 435
4 inch	$278 - $541
3 inch	$340 - $592
2 inch	$325 – $584

Acquisition services vary by imagery provider

Assuming an average size county (i.e., 840 square miles) in Nebraska wanting full coverage of a 4 inch oblique imagery. This would equate to $344,400 for that county for the acquisition of oblique imagery.

Historic Aerial Photography

The RFI did not capture information in regards to costs associated to scanning, digitizing and orthorectification of historical imagery. These costs will be sought in a separate implementation plan.

Minimum Cost Estimates for a Statewide Orthoimagery

The recommendations of this business plan is to support the primary orthoimagery product. Costs for other add-ons and buy-ups are additional and would be covered by those entities interested. The program would still provide the necessary coordination and procurement for those services. Table 4 represents estimated costs for the Nebraska Statewide Imagery Program.

Table 4. Total estimated costs for the Nebraska Statewide Imagery Program.

Activity	Year 1	Year 2	Year 3	Year 4	Year 5
Orthoimagery Acquisition and Processing Including: Quality Assurance / Quality Control	$1,780,000		$450,000		1,780,000
Distribution and Hosting	$6,400	$6,400	$6,400	$6,400	$6,400
Program Management / Support	$25,000	$10,000	$25,000	$10,000	$25,000
Total	$1,811,400	$16,400	$481,400	$16,400	$1,811,400

Years 1 and 5 are assuming statewide coverage of orthoimagery. Year 3 is assuming 25% coverage of urbanized and other prioritized areas in the state. This amounts to a cost on the order of $23.42 per square mile. The costs associated during Years 2 and 4 are due to ongoing data hosting and distribution and contract preparation for successive year collections and ongoing buy-ups.

5.8 Finance and Procurement Strategy

The statewide imagery program is based upon partnerships between state, county and federal sources. This consortium of partners, seek an annual acquisition program that is continuously funded. However, funding for the overall program is still contingent upon the availability of state, county, local, federal, and other funding from year to year. The national trend in funding statewide imagery programs has been an accumulation of partners at the local and state government level. Involving a consortium of partners at the state level builds capacity and instills competitiveness among the orthoimagery service industry. This further promotes competitive and affordable prices, high quality products, and timely services for large orthoimagery projects.

5.8.1 Funding Sources

Funding for a statewide imagery program depends on budgeting, planning, negotiating, and factors that may not be apparent. As a framework, the recommended funding strategy for the statewide program is to work with the following groups to obtain funding that will support the recommendations contained in this plan. This framework involves imagery acquisition, data access and distribution, program management and investment in geodetic control.

1. ***State agencies and statewide organizations, including the 9-1-1 Board on behalf of local operations, that use state funds and apply geospatial data to business processes.*** Specific amounts depend on project locations in relation to state program requirements, restrictions, timing and budgets.
2. ***Local governments.*** Specific amounts depend on project locations in relation to local program requirements and availability of funds.
3. ***Other political subdivisions and organizations, including electric power districts, natural resource districts, and other governed districts.*** In partnership with public entities, political subdivisions and organizations are potential sources for cost-share in selected counties where those groups have business requirements for current high resolution imagery.
4. ***Federal organizations, including cooperative agreements led by the Federal Geographic Data Committee.*** Funding from federal organizations depends on project locations, federal program initiatives and requirements, availability of funds, and limitations based on location and purpose.

State Funding

This business plan recommends state agencies and existing sources of funds (i.e., those created by statute that have relevance) are used to support the base orthoimagery product for the state. The other option is that an existing or new state appropriated fund is enhanced or created to support the NESDI data layer development and distribution of data. A majority of states in the nation are funded through 9-1-1 boards, local contributions and state agencies. Nebraska has a legislative appropriated Universal Service Fund Act, where many counties are funding several geospatial data sets to support enhanced 9-1-1 operations.

At the time of writing this business plan, there are decreases in revenues at the state level. State agencies have been asked to reduce their budget submissions so that core operations and business functions are met. The state agencies have already submitted their next biennium budgets for fiscal years 2018-2019. In order to get orthoimagery acquisition into those budgets, a specific request would need to be submitted to the Governor's office or funding allocated through legislation in early 2018.

The success of this imagery program depends on state level funding. Participating state agencies and stewards of state appropriated funds may want to begin addressing this data in their budgets moving forward. State Agencies that have participated in imagery projects in the past include Nebraska Department of Roads and the Nebraska Department of Natural Resources.

Additional imagery product and services that go beyond the primary orthoimagery data layer can be purchased by entities having needs for those to support their applications (i.e., oblique imagery, increased resolution of orthoimagery, UAS).

Local Funding

Many of the larger metropolitan cities and counties have routinely purchased orthoimagery and oblique imagery on an ongoing basis. Current funding for these products has relied mainly on local budgets. Although funding may not be consistent and reliable across the state, and although products specifications do not meet state standards, there are steps that can be taken to ensure all funding opportunities are pursued.

Local governments are the source for most of our geospatial data layers. It is important to recognize this role. Applications to support property assessment and public safety rely on orthoimagery and other products such as oblique imagery. There are political subdivisions that work with multiple municipalities and counties across the state. Public Power Districts have a need for high-resolution orthoimagery for utility planning. Natural Resources Districts have a need for imagery for water management regulation and monitoring.

Local governments and political subdivisions will not be able to support the program by itself due to inequality of budgets and timing. However, they can be a source of funding when supporting the core orthoimage product, if and when, the state funding options are limited.

Having the core orthoimagery product covered for all municipalities and counties frees up local and political subdivision budgets to support value-added imagery products such as oblique imagery.

Federal Funding and Grants

Some state agencies currently receive federal funding as part of their business model. The Nebraska Department of Roads receives funding from the Federal Highway Administration for various projects including GIS framework data and occasionally funding is set up in federal budgets to specifically target data acquisitions. There will be inquiries to other state agencies to determine if any existing federal funding is suited for acquisition of orthoimagery. Other federal agencies that might potentially

contribute to a Nebraska imagery program include US Army Corps of Engineers and the Federal Emergency Management Agency.

Federal funding can be requested through Nebraska's U.S. Senators. These funding requests are made annually to the Senators office where all requests are compiled and evaluated. If approved, the Senator includes it in their budget request through the appropriate committee. This process usually begins early in the year in hopes of including it in the final budget which is usually approved at the end of the year. Once the request is in the approved budget, the appropriate federal agency is notified and the grant process begins. Project summaries, proposals, details, and budgets are required to be submitted through the grants online process. After approval, the grant is awarded and work typically begins at the beginning of the next fiscal year. This entire process can take as little as 18 months, or it could take years. Project proposals for this program will be developed and submitted for consideration before February of 2018 to be considered in the 2019 budget.

Occasionally there are federal grants advertised for data acquisition. This process goes through the Federal Grants service which oversees all grant funding for the federal government. This office provides the notifications about the requirements and terms of the grant, oversees the application and review process, and manages the reporting and funding. Without prior notice, the time frame for submission of all material is usually short, so enlisting staff with prior grant writing experience must be utilized to ensure deadlines are met and the state has a reasonable chance of securing grant funds. Existing personnel resources with grant writing experience within state government will be enlisted to provide assistance.

5.8.2 Fiscal and Procurement Management

A coordinated procurement process will cut down on the inefficiency of multiple procurements for the same type of data and services within a jurisdiction and across jurisdictions. To achieve this efficiency, it is recommended that the fiscal authority and management of funds for procuring imagery products and services will need to be supported within the OCIO and Nebraska Department of Administrative Services.

The OCIO is located within the Department of Administrative Services (DAS) which provides administrative and budgetary services for the office and other state agencies and partnering entities. The OCIO provides overall IT policy, governance, planning and oversight, IT coordination for state agencies, and development, oversight, and operation of enterprise shared systems.

The Geographic Information Officed within the OCIO will be responsible for coordination of funds, facilitating procurement and participate in management of the program to assure deliverable products meet procurement requirements. This effort is currently led by the State GIS Coordinator for similar statewide geospatial data programs.

The OCIO can provide the necessary administrative support to handling contracts, procurement and follow through on acquisition products and services. Other state agencies and partners through the program management team will participate in the management and decisions made for fund allocations towards the Nebraska Statewide Imagery Program.

Once initial steps are in place for identifying partners and source of funds, the OCIO Geographic Information Office can initiate the process for coordinating funds and initializing the acquisition process of services. They can also establish agreements with other state funded entities in this process to acquire cost sharing of funds.

The fiscal and procurement process will need to address several issues identified by our partners prior to finalizing an acquisition plan. The following are some of the needs to address for an effective fiscal and procurement process to occur:

- Documented and communicated procurement steps with timelines to allow partners to plan, budget, procure, and accept delivery of products and services.

- Designated customer service at DAS and OCIO to support ongoing questions and assistance to fulfill purchases.
- Ability to select from several vendors depending on the application requirements.
- Ability to pay for products and services over several years.
- Flexibility for finance and procurement of product and services among partners with varying fiscal year start and end dates.
- Ability to choose from various add-on products and services at different times than the overall orthoimagery acquisition product timelines.
- Ability to readjust procurement process if it does not meet partner needs and requirements.

5.9 Reduction of Risk

It is important to identify potential risks prior to implementing a large scale program such as the Nebraska Statewide Imagery Program. Risks are typically associated to financial, organizational, and technical aspects to any program. By identifying these types of risks before they arise in program, it can speed up the process for remediation or corrective action before costs and efficiencies become difficult to manage.

Financial Risks

Financial risks can be associated with sustaining the allocation of funding and resources for imagery implementation work. This includes internal decisions inside partner organizations that impact funding streams and timing, external economic changes that impact resources, and potential problems with implementation, planning or management resulting in over budget of projects.

Coordinating funding under these conditions can be challenging and must be proactive to be effective. One of the main challenges is reducing risk in the timing and allocation of resources across varying start times and fiscal year budgets. Potential partners will have different budget processes and timelines. Budgets range from one to two year cycles and start dates differ during the year depending on the government entity. The federal fiscal year runs from October 1st until September 30 of the following year. State Agencies maintain a two-year budget cycle and the state fiscal year runs from July 1st until June 30th of the following year. Political subdivisions and counties run similar fiscal years as the state but budget for one year at a time. Counties and cities may have similar or different budget processes. Funds may become available from one source as the opportunity for funding from another source closes.

The following are additional examples of financial risk:

- Sustainable funding over time does not materialize. Local governments may become dependent on state-funded orthoimagery acquisition and may not be prepared when state program funds are not available.
- Insufficient internal funding allocation or funding diverted to other projects
- Expected external funding does not materialize
- Dedicated vendor services and internal staff resources not sufficient
- Cost projections do not meet actual costs
- Poor contractor performance results in increased costs

Organizational Risks

Organizational risks involve the organizational, political, or legal aspects of imagery acquisition and delivery of products. This includes all aspects of partner organizational relationships, management, staff assignments, governance structure, high-level legislative and executive support, legal and policy rulings, and all types of political and media influences on implementation work.

The following are a few specific examples for this program:

- Expected legislative support is not provided
- Lack of sufficient senior executive awareness and support at various partner levels
- Expected level of participation from stakeholder groups is not delivered
- Administrative delays in procurement and policy approval of organizational/legal obstacles in forging formal partnerships
- Contract discrepancies impact timing and quality of contracted work
- Poor management and coordination creates delays and obstacles to consensus
- Political battles reduce level of collaboration and joint project participation
- Inability to build trusted relationship with the geospatial user community

Technical Risks

These risks are associated with the technological and operational aspects of the program, including procedural workflows associated with imagery acquisition and technology infrastructure to support delivery and distribution of data. These risks reflect potential technical obstacles in the program's development and implementation plans that could impact costs or the schedule.

The following are a few specific examples for this program:

- Weather conditions limit the number of days and hours suitable for capturing aerial exposures that meet specifications for sun angle, cloud-free skies, and leaf-off conditions.
- Natural disasters, particularly flooding, may obscure ground features.
- Delays in adhering to technical standards to be used as basis for imagery acquisition and data delivery.
- Problems with information technology infrastructure to support dissemination and delivery of imagery products.
- Network communication performance limitations impact access to imagery data and services.

6.0 Implementation Plan

6.1 Implementation Details and Timeline

The success of the Nebraska Statewide Imagery Program will be realized when certain objectives have been met. The following is a summary of activities that support the accomplishment of each program objective. The figure in Appendix III represents a timeline for the first four years of when objectives begin and end for the program.

1.0 Establish a program management team and operations plan with administrative coordination from the Geographic Information Office within the Office of the Chief Information Officer.

The expectation for the team is to have participants be in their role for the first two years. Thereafter, team members can rotate on an annual basis if they choose. The important thing is to maintain representation across all stakeholders. The formation of the planning team and development of an operations plan will begin as soon as the business plan is approved. This is a voluntary team of members. The State GIS Coordinator will solicit volunteers to be on the team that will include state, county, city, University and federal government individuals who have vested in interest in the imagery program.

The first meeting of team members will be to develop operational plans including a procurement plan. This will lead into a request for proposal (RFP) and outline methods to communicate the business plan objectives to stakeholders.

Start Date: February 2017
Duration: 5 months development, and implementation ongoing. After two years, new members can rotate annually during February.

2.0 Establish and maintain standards, policies and strategies to emphasize cooperation and coordination among state, federal, county, municipality, utilities, university and other political subdivisions and organizations.

The process will begin by defining the partners and relationships that exist between local, state and federal agencies. Areas of agreement will be identified and incorporated into strategies and policies to guide the program in order to promote cooperation.

Standards for orthoimagery acquisition have already been completed. However, with changes in technology and usage in applications, it may require these standards to be updated over time. Existing policies and procedures will be documented with timelines for the procurement and acquisition process.

Start Date: January 2017
Duration: 9 months development, and implementation/modifications ongoing

3.0 Identify and develop funding sources for program implementation and long term sustainability.

Initial funding for the first statewide orthoimagery acquisition and sustainable funding long term for orthoimagery are two of the strategies to address for this program. The program management team will further define funding from state, local and federal sources so they can be communicated to get necessary commitments from stakeholders. This will become important for budgeting, identify potential risks upfront, and be able to adjust the program in times of economic downturn.

The NITC GIS Council and OCIO need to work with the current administration and legislation to obtain a budgetary line item that will be sufficient to cover the anticipate annual costs. Once a budgetary program is in place then the OCIO will initiate a procurement process to purchase photogrammetric services covering the necessary acquisition cycles, project phases, and allowing for additional buy-up provisions from the program. Additional strategies and approaches for this objective are further outlined in section 4.8.Finance and Procurement Strategy.

Start Date: February 2017
Duration: 9 months development, and implementation ongoing. Planning efforts are re-evaluated during times of annual budgeting between June through September.

4.0 Implement a procurement and vendor selection process that allows multiple levels of government, university and other political subdivisions to purchase imagery and related products.

Program partners interested in participating in the program will be identified and specific information about their needs and funding processes will be documented. A Request for Information (RFI) was conducted in 2015 to obtain cost estimates as it relates to statewide imagery acquisition and data hosting services. The RFI provided information about additional buy-up options of imagery including oblique imagery, data hosting, and map services.

The program management team will further summarize needs of partners and the RFI information

along with strategies in the acquisition plan to develop a Request for Proposal (RFP). Depending on the scope and procurement issues there could possibly be several RFPs outlined for the various products and services needed. The RFPs will outline clear specifications and requirements for imagery acquisition and obtain updated costs in order to choose appropriate services from the contract. The members of the program management team will serve as evaluators for selecting contractors. They will follow DAS policies and procedures when selecting vendor contract awards. Once funding is secured, State of Nebraska DAS purchasing and OCIO will issue the RFP and then initiate contracts to selected contractors.

The RFP for orthoimagery acquisition will be constructed to allow only one award for the first acquisition event, with contingency to extend to multiple years if needed. This allows for the procurement process to be readjusted without being locked into a long-term contract that is difficult to modify or end.

Initial flight planning meetings will be required with contractors prior to data acquisition. This will be outlined in the RFP requirements. The program management team along with partners involved in the program will have the opportunity to evaluate products and services prior to accepting final delivery of the contract. Once the final products are delivered the OCIO will work with distribution activities outlined in objective 6.

Additional strategies and approaches for this objective are further outlined in section 4.8.Finance and Procurement Strategy.

Start Date: April 2017
Duration: 6 months development and implementation efforts are set in advance to flight acquisitions in fall and/or spring of each year.

5.0 Develop and implement a preservation plan for the digital conversion and archiving of historical aerial imagery.

This objective will need to be further defined in order to outline the information requirements and best practices for preserving historical aerial photographs. The Conservation Survey Division at UNL and the OCIO Geographic Information Office will lead in the development and implementation plans for this objective. There are several processes in the plan that will need to be considered. At a minimum, this involves indexing, rectification, attribution, metadata documentation, and distribution in order to deliver quality historical imagery.

Indexing

Tabular Index
Imagery will be indexed in a tabular format, referencing all significant areas/portions of the image in a table by section, township, and range and any other useful agency-specific grid system. This level of indexing does not require scanning.

Generalized Spatial Index
Create a spatially-referenced, generalized bounding box that represents the approximate boundaries of the imagery which can be represented within and searched for within a GIS. This process can be done with or without scanning of imagery.

Geo-Referencing and Rectification

Geo-Referenced
Imagery must first be scanned for this level of indexing/rectification. Guidelines and best practices will be used or developed where necessary for proper scanning of aerial photographs. It will require spatial coordinates on a minimum of four points that have a reasonable distribution

around the image. Geo-referencing steps may vary if one's end goal is a standalone, geo-referenced image (with collar info) or mosaic imagery.

Suggested reference material to be used for geo-referencing

1. Best available imagery
2. PLSS
3. 7.5 minute topo quad maps
4. Metadata to be used to record reference material used in geo-referencing

Ortho-rectification

Imagery must first be scanned. Requires information on several parameters of imagery to accurately complete the process (e.g., altitude, DEM, camera focal length)

Attribution

Proposed Attribution for Historic Imagery and/or Maps

- Document reference (number or ID on imagery or map)
- Document Year
- Media Type of original document. This includes a possible choice between aerial imagery film, aerial imagery enlargement on paper, aerial imagery enlargement on mylar, paper maps, and other document types.
- Color of imagery: B/W, color, infrared
- Physical size of original
- Approximate scale of original document
- Approximate geographic location of image
- County
- Section, Township, Range
- Map Index? Y/N
- Index Name (if available)
- Original Project Name
- Original Project Date
- Date inventory information collected
- Contact info for custodian of original
- Current storage location of orginal

Proposed Attribution as Historic Imagery and/or Maps are Scanned

- Document reference (number or ID on imagery or map)
- Scanning resolution
- Scanning parameters (if available)
- Date of scan
- Scanning vendor
- Scan file name
- Contact info for custodian of scanned document

Distribution

The distribution of imagery will include provisions for cataloging and indexing data files through NebraskaMAP. The indexing and metadata will be required for this activity.

Start Date: April 2017
Duration: 3 months development and implementation ongoing.

6.0 Expand existing data sharing and distribution methods to leverage historical and newly acquired imagery products so they are accessible, both publicly and for secure uses.

Imagery data must be easily accessible to the community of users to achieve the highest return on investment. Current imagery data sets are continuing to be cataloged and registered within the State of Nebraska Geospatial/GIS Enterprise platform and extended through NebraskaMAP. Additional geoprocessing tools to enable analysis and downloading of large raster files are under development and will start to be released in the fall of 2017.

The primary data hosting for raw tiles, cached, and/or mosaic of the orthoimagery files will be through the State of Nebraska Geospatial/GIS Enterprise platform. The Conservation Survey Division at UNL will continue to host the satellite and historical imagery through their programs. The state's enterprise solution can catalog imagery data holdings in other locations so it can be leveraged through NebraskaMAP and other application viewers. The OCIO will work with the University of Nebraska to develop methods to connect users to data with little, to no, data duplication.

Imagery products are large in size and are costly for ongoing hosting of the data. Efforts are underway by the State to outsource large raster files such as imagery to third party cloud hosting solutions. Ongoing efficiencies will be implemented to reduce costs in data hosting and application technologies. Other techniques using Enhanced Compression Wavelet (ECW) or Mr. SID formats for data compression will also be used in the process.

There are additional methods that will be addressed to distribute and consume imagery products. The following are some examples for this objective:

- Online image services map viewer for allowing visual quality control of the processed imagery before physical delivery of the final product
- Implement an online map viewer to show existing coverages of all imagery data products
- Provide server-based map services to allow partners to connect to data through desktop and other online map applications
- Online geoprocessing tools to further analyze and develop derivatives from imagery such as change detection and land use classifications.
- Appropriate web-based plug-ins or APIs to allow users to view, rotate and make measurements with oblique imagery
- Imagery products are registered and cataloged within NebraskaMAP so that users can quickly search and find data on a map.

Start Date: January 2017
Duration: 9 months development, and implementation ongoing.

7.0 Provide communications, technical assistance and education outreach activities supporting the efficient utilization of imagery products.

The existing relationships between the members of the NITC GIS Council and program partners will be used as the foundation for communications. Communication of standards, guidelines, and procedures from the state level will be incorporated into the existing county organizational structure. Modifications to this process will include incorporating data standards that meet wider audience needs. This will encourage county government to collaborate with entities around their county. This feedback will assist in updating the existing contracting process to ensure all contracts include the requirements needed for their applications. Meanwhile, these efforts support the data standards, procedures, and scope of work needed to meet the goals of the program.

Specific strategies to support communications, technical assistance and education outreach activities are located in section 7.0 Communications and Outreach.

Start Date: October 2017
Duration: 4 months development and implementation ongoing.

8.0 Develop and implement an acquisition plan for statewide orthoimagery coverage and other products targeted for data collection beginning the spring of 2018.

This plan will focus on the first year of orthoimagery and other imagery deliverables set for the spring of 2018. This is assuming we have funding sources and the procurement process in place. Input on product and service needs will be gathered early on from local, state and federal governments interested in partnering in the program. The plan will include a RFP, and procurement steps will be established to accept bids and award contracts as outlined in Objective 4. The plan will outline starting areas to begin flight acquisition, estimated costs from partners, procurement and agreement deadlines, acceptance of deliverables for review, and approval of deliverables. Municipalities and high priority areas wanting additional add-on products will be organized to assure efficient flight plans by the contractor.

The acquisition plan will be reviewed by all funding partners to assure accuracy prior to the initial flying season. Specific processes and timelines for procurement and acceptance of deliverables will be communicated at various steps. The program management team will conduct face-to-face meetings, webinars and develop other print materials to support communication during these steps. On an ongoing basis, the process will be repeated and all acquisition plans will be formally presented to any potential state, federal, or local partners as early as possible to encourage feedback, comments, and any information about potential funding.

Start Date: January 2017
Duration: 9 months development, and implementation fall and/or spring of every two years on a cycle.

9.0 Conduct a biennial evaluation and make necessary programmatic adjustments to procurement, standards, and other processes that impact activities and outcomes of the program.

The program management team will lead an assessment of the program. It will document how each of the objectives were met, lessons learned, and provide appropriate recommendations to readjust the overall program. A questionnaire will be developed to facilitate data gathering internally and an online survey will be used to monitor feedback from other stakeholders involved in the process. This information will be compiled into a biennial report and will be submitted to the NITC GIS Council for review and further recommendations in the fall every two years. Specific desired outcomes that will be assembled and evaluated are further outlined in section 8.0 Measuring Success and Feedback for Recalibration.

Start Date: October 2018
Duration: 2 months development, and ongoing modifications until development starts again in two years.

7.0 Communications and Outreach

7.1 Communications

Develop a communications plan through the program management team by incorporating some of the following objectives:

- Establish necessary branding and overall message that can be marketed to a wide variety of audiences at the local, state and federal levels.
- Maintain a comprehensive contact database of partners including government, associations and industry that may benefit from imagery products.
- Develop a web-based coverage map through NebraskaMAP showing imagery data availability across the state.
- Share impact statements aimed at key decision makers who are managers, directors and elected officials at the federal, state and local levels showing impact and uses of the data through the program and how benefits outweigh program costs.
- Develop other explanatory and promotional materials that provide information on needs, applications, and benefits of the program to users of the data.
- Provide timely face-to-face meetings, webinars, and teleconferences for partners to respond to and provide input on imagery acquisition opportunities as they become available.
- Maintain a statewide electronic mailing list for emailing frequent communication, news, and updates about imagery acquisition among partners. Use other electronic social media and web sites to also communicate information.
- Conduct presentations, seminars, lectures, posters and displays at various statewide association and other meetings where appropriate. A few example meetings and conferences can include:
    - Nebraska GIS LIS Association Biennium Symposium
    - Annual Water Symposia conducted by the Nebraska Water Center
    - Annual meetings and conferences for Nebraska Association of County Officials (NACO), League of Nebraska Municipalities, Nebraska Association of Resources Districts (NARD), Natural Resources Districts, Soil and Water Conservation Society, Nebraska American Water Works Association (AWWA), American Public Works Association (APWA), Nebraska Water Environment Association (NWEA), other Water Resource related associations, United States Geological Survey, Natural Resources Conservation Service, Federal Emergency Management Agency, and Army Corp of Engineers.

7.2 Technical Assistance and Education Outreach

Develop a technical assistance and education outreach plan through the program management team by incorporating some of the following objectives:

- Identify appropriate target audiences and package promotional, educational, and technical assistance materials to support their needs.
- Develop illustrative content for use in both printed and web based media.
    - Fact sheets
    - Technical “How-To” guides
    - Electronic presentations made available as either stand alone or through web-based communication such as webinars.
- Partner with University of Nebraska entities that are in line with our program goals to assist in facilitating and conducting educational activities across the State. For example, leverage groups such as NebraskaView, Center for Advanced Land Management Information Technology (CALMIT), and Extension Service.

- Develop and implement hands-on workshops on how to use imagery data through various applications such as GIS and other mapping and interpretive software.
- Support technical assistance needs of users by providing them connectivity to a statewide expert list of volunteers who manipulate and use imagery data for a variety of applications. This group would be listed as a contact list on the NebraskaMAP web site for assistance.

8.0 Measuring Success and Feedback for Recalibration

The successful implementation of this business plan should manifest itself in realization of a statewide imagery program to support multiple products of sufficient quality to support the majority of Nebraska's needs. As the most current and the most accurate imagery products are provided, it would constitute the authoritative imagery products for Nebraska. As such, it would be carefully managed, systematically improved, and widely distributed. To ensure that imagery efforts are bearing fruit, the imagery project management team would assemble and evaluate the following specific elements of success:

1. State standards and guidelines are developed for Nebraska imagery products and adopted by the NITC
2. Core imagery requirements are identified and documented to aid in the selection of imagery products to pursue
3. Awareness of the importance of imagery data in local, regional, state, and federal activities and in the activities of private concerns is elevated resulting in an increase in appreciation and support of statewide imagery efforts.
4. A statewide imagery program is authorized and funding aligned by the stakeholders.
5. Acquisition, marketing and outreach, stewardship, and distribution plans are written to guide the imagery program into the future.
6. Imagery projects resulting in statewide imagery coverage are systematically and efficiently executed.
7. Historical aerial photographs are preserved digitally meeting standards.
8. Imagery investments are leveraged by stewardship and distribution of the data is made available through NebraskaMAP.

The imagery program management team will identify specific actions for recalibration of the implementation of this plan as needed. This will be accomplished from ongoing feedback of program participants, the evaluation of objectives being met, and overall maturity of the program based on sustainable funding and return on investment.

9.0 References

American Society of Photogrammetry and Remote Sensing (ASPRS). 2014. ASPRS Positional Accuracy Standards for Digital Geospatial Data. Photogrammetric Engineering & Remote Sensing, Vol. 81, No. 3. Edition 1, Version 1.0. – November, 2014. http://www.asprs.org/wp-content/uploads/2015/01/ASPRS_Positional_Accuracy_Standards_Edition1_Version100_November2014.pdf

National Emergency Numbering Association (NENA). 2007. 02-014 NENA GIS Data Collection and Maintenance Standards. http://c.ymcdn.com/sites/www.nena.org/resource/collection/C74A8084-E3BD-405D-93C2-48AFCFA5B490/NENA_02-014-v1_GIS_Data_Collection_and_Maintenance.pdf

National States Geographic Information Council (NSGIC). 2012. Justifying the Cost of Authoritative Imagery. https://www.nsgic.org/public_resources/NSGIC_Justifying_Cost_of_Imagery_102612_Final.pdf

NebraskaMAP. 2016. Data and Content Management Policy. https://www.nebraskamap.gov/data-and-content-management-policy

NITC. 2005. NITC 3-201 Geospatial Metadata Standard. Nebraska Information Technology Commission GIS Council. http://nitc.ne.gov/standards/3-201.html

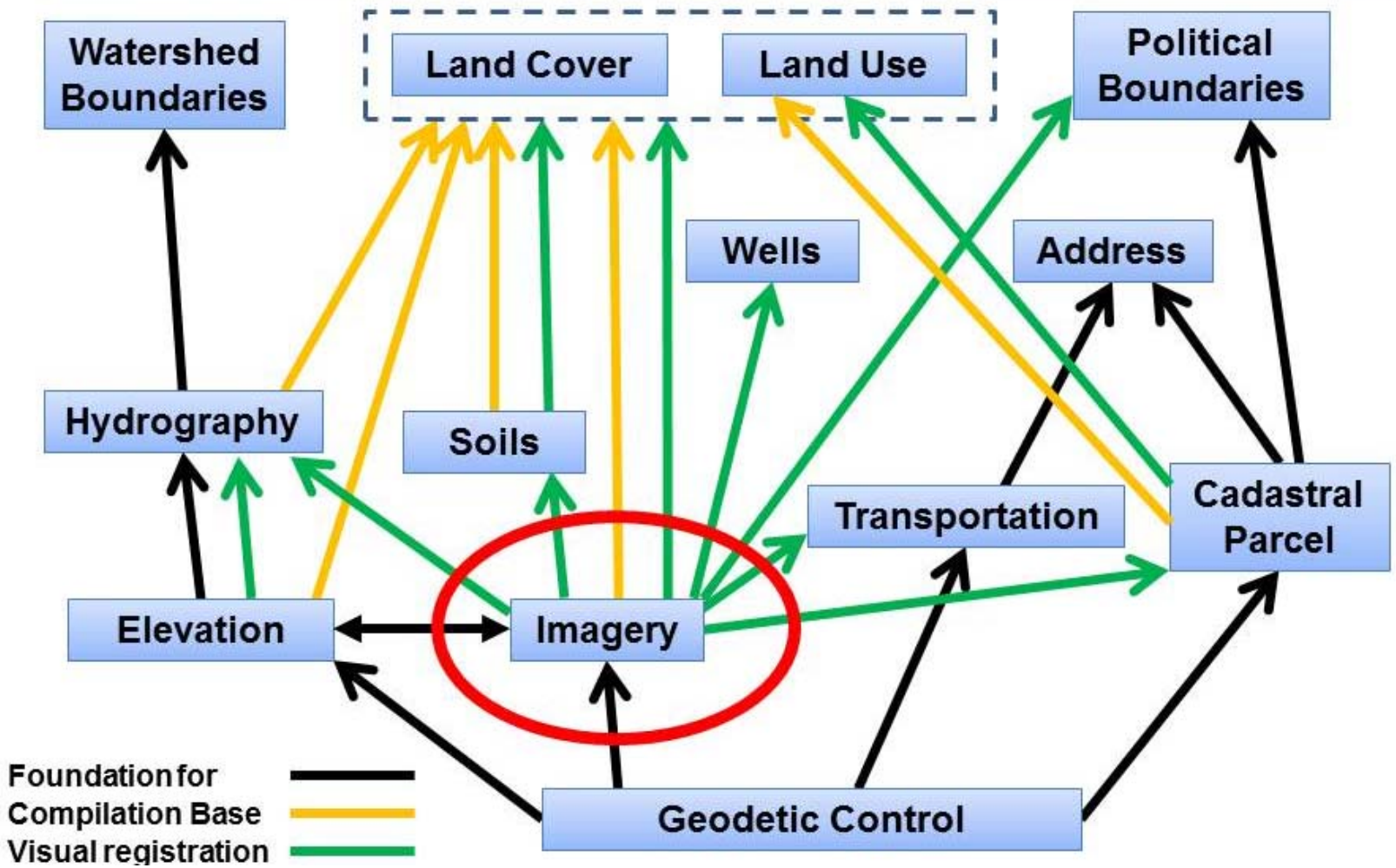
NITC. 2014. NITC 3-203 Elevation Acquisition using LiDAR Standard. Nebraska Information Technology Commission GIS Council. http://nitc.ne.gov/standards/3-203.html

NITC. 2014. NITC 3-204 Imagery Standards. Nebraska Information Technology Commission GIS Council. http://nitc.ne.gov/standards/3-204.html

NITC GIS Council. 2016. Nebraska Statewide Imagery Program, Imagery Working Group Charter. http://nitc.ne.gov/gis_council/workgroups/imagery/documents/ImageryCharterGISCouncil.pdf

USDA/USGS. 2007. Imagery for the Nation Cost Benefit Analysis. 90 pages. https://www.nsgic.org/public_resources/Imagery_for_the_Nation_IFTN_CBA.pdf

Appendix I – Relationship of Imagery to other Nebraska Spatial Data Infrastructure Layers

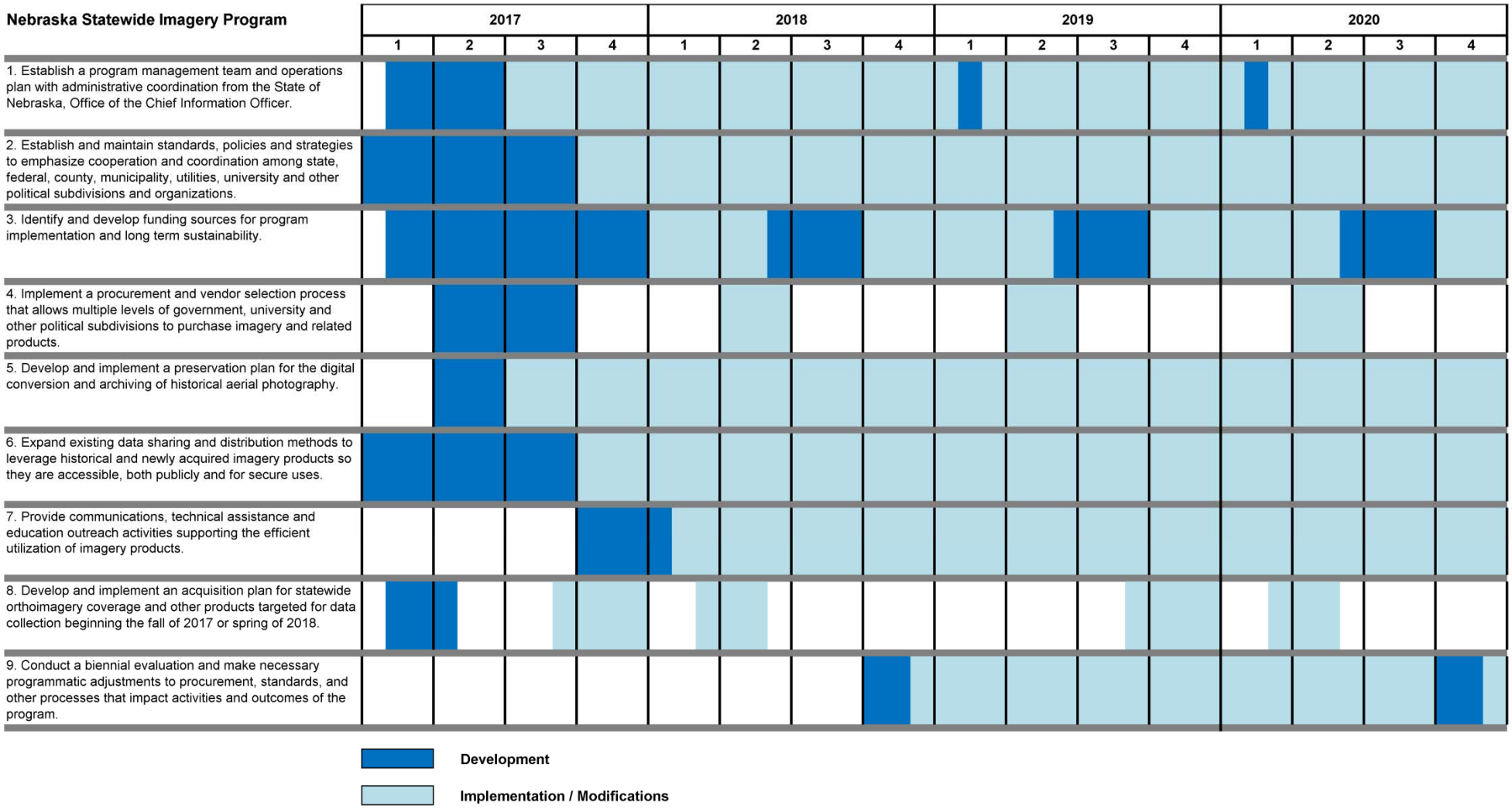


Appendix II – Orthoimagery Applications and Feature Recognition Examples by Resolution

Ortho-Imagery Applications and Feature Recognition by Resolution

	3-4 Inch	6 Inch	1 Foot	0.5 Meter	2 Foot	1 Meter
Applications	Utilities Engineering Roadside Feature Inventory	Central Business District (CBD) Mapping Public Works Management Transportation Engineering Urban Forestry	Urban Municipal Mapping Traffic Control Management	Urban Municipal Mapping Bridge Maintenance Large structure damage assessment	Semi-Urban Mapping Parks and Recreation Management	General Land Cover and Vegetation Type Identification Rural Mapping Mapping Large Scale Storm Debris
Identifiable and Measurable Features	Utility Boxes Fire Hydrants Reflective Road Markings Parking Meters Golf course flags Power and Communication Lines	Road Centerlines Culverts Manholes Train Tracks Fence Posts	Turning Lanes Marked Pedestrian Crossings Speed Bumps Fences Park Benches Communication Towers	Sidewalks Nature Trails Overhead Rail Bridges Housing and Roof Structures Cattle Guard Crossings	Driveways Medians Bike Lanes Car Ports Sheds	County and Gravel Roads Railroads Alleys Trees in Sparse Areas Stock Ponds Wind Turbines Large Commercial and Livestock Buildings with Add-ons

Appendix III – Implementation Timeline



Attachment 4-e-i-1

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 17-02
Final

A PROPOSAL TO REVISE NITC 1-101 relating to definitions; to modify the basic format of the definitions; to amend various definitions; to add new definitions; and to repeal the original section.

Section 1. The following provisions constitute a revised section 1-101:

1~~. General Provisions~~1-101 General definitions.

~~For purposes of the NITC Standards and Guidelines documents, the definitions found in this document apply. Some NITC Standards and Guidelines documents may contain additional definitions which will only apply to the document in which they appear.~~ Subject to additional definitions contained in subsequent articles which are applicable to specific articles or parts thereof, and unless the context otherwise requires, in the NITC Technical Standards and Guidelines:

~~**2. Definitions**~~

1. "Agencies, boards, and commissions" has the same meaning as agency.

2. "Agency"~~: Any~~ means any agency, department, office, commission, board, panel, or division of ~~the state~~state government. [Source: based on Neb. Rev. Stat. § 81-2402(1)]

~~Agencies, Boards, and Commissions: Agencies, Boards, and Commission has the same meaning as "Agency."~~

3. "Agency information security officer" means the individual employed by an agency with the responsibility and authority for the implementation, monitoring, and enforcement of information security policies for the agency.

4. “AISO” is an abbreviation for agency information security officer.

5. “Authentication”~~: The~~ means the process to establish and prove the validity of a claimed identity.

6. “Authenticity”~~: This is~~ means the exchange of security information to verify the claimed identity of a communications partner.

7. “Authorization”~~: The~~ means the granting of rights, which includes the granting of access based on an authenticated identity.

8. “Availability”~~: The~~ means the assurance that information and services are delivered when needed.

9. “Biometrics”~~: Refers to~~ means the use of electro-mechanical devices that measure some physical, electrical or audio characteristic of an individual and make use of that specific measurement to verify identity.

10. “Breach”~~: Any~~ means any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

11. “Business ~~Risk~~risk”~~: This is~~ means the combination of sensitivity, threat and vulnerability.

12. “Chain of ~~Custody~~custody”~~: Protection~~ means the protection of evidence by each responsible party to ensure against loss, breakage, alteration, or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

13. “Change ~~Management Process~~management process”~~: A~~ means a business process that ensures that no changes occur on a computing resource without having gone through a methodology to ensure that changes will perform as expected, with no unexpected repercussions.

14. “Chief Information Officer”~~ (CIO): Chief Information Officer~~ means the Nebraska state government officer position created in Neb. Rev. Stat. § 86-519.

15. “CIO” is an abbreviation for Chief Information Officer.

16. "CJI" is an abbreviation for Criminal Justice Information, the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII. [Source: *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.6, 06/05/2017]

17. "CJIS" is an abbreviation for Criminal Justice Information Services Division, the FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies. [Source: *Criminal Justice Information Services (CJIS) Security Policy*, Version 5.6, 06/05/2017] See also "CJI."

18. "Classification"~~: The~~ means the designation given to information or a document from a defined category on the basis of its sensitivity.

19. "Commission" means the Nebraska Information Technology Commission.

20. "Communications" means any transmission, emission, or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, radio, optical, or other electromagnetic systems. [Source: Neb. Rev. Stat. § 81-1120.02(4)]

21. "Communications system" means the total communications facilities and equipment owned, leased, or used by all departments, agencies, and subdivisions of state government. [Source: Neb. Rev. Stat. § 81-1120.02(3)]

22. “Compromise”~~: The~~ means the unauthorized disclosure, modification, substitution, or use of sensitive information, or the successful action to invade system by evading its security. For example, a computer had been compromised when a Trojan horse has been installed.

23. “CONFIDENTIAL” (written in all capital letters) means the data classification category defined in section 8-902.

24. “Confidentiality”~~: The~~ means the assurance that information is disclosed only to those systems or persons that are intended to received that information.

25. “Continuity of ~~Operations~~ operations ~~Plans~~ plan”~~(COOP): Provides~~ means a plan that provides for the continuation of government services in the event of a disaster.

26. “Controls”~~: Countermeasures~~ means countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

27. “COOP” is an abbreviation for continuity of operations plan.

28. “Critical”~~: A~~ means a condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

29. “Cyber ~~Security~~ security ~~Incident~~incident”~~: Any~~ means any electronic, physical, natural, or social activity that threatens the confidentiality, integrity, or availability of ~~State of Nebraska~~state information systems, or any action that is in violation of the Information Security Policy.

For example:

- Any potential violation of ~~Federal~~ federal or ~~State~~ state law, or NITC policies involving ~~State of Nebraska~~state information systems.
- A breach, attempted breach, or other unauthorized access to any ~~State of Nebraska~~state information system originating from either inside the ~~State~~ state network or via an outside entity.
- Internet worms, Trojans, viruses, malicious use of system resources, or similar destructive files or services.
- Any action or attempt to utilize, alter, or degrade an information system owned or operated by

the ~~State of Nebraska~~state in a manner inconsistent with ~~State~~ state policies.

- False identity to gain information or passwords.

30. “Data”~~: Any~~ means any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media, including all records as defined by the Records Management Act. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

31. “Data ~~Security~~security”~~: The~~ means the protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

32. “Data ~~Owner~~owner”~~: An~~ means an individual or a group of individuals with responsibility for making classification and control decisions regarding use of information.

33. “Denial of ~~Service~~service”~~: An~~ means an attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

34. “Disaster”~~: A~~ means a condition in which information is unavailable, as a result of a natural or man-made ~~occurrence, that~~occurrence that is of sufficient duration to cause significant disruption in the accomplishment of the ~~State of Nebraska~~state's business objectives.

35. “DMZ”~~: Demilitarized~~ is an abbreviation for demilitarized zone~~;~~, and means a semi-secured buffer or region between two networks such as between the public Internet and the trusted private ~~State~~ state network.

36. “Encryption”~~: The~~ means the cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

37. “Enterprise”~~: Enterprise~~ means one or more departments, offices, boards, bureaus, commissions, or institutions of the state for which money is to be appropriated for communications or data processing services, equipment, or facilities, including all executive,

legislative, and judicial departments, the Nebraska state colleges, the University of Nebraska, and all other state institutions and entities. [Source: Neb. Rev. Stat. § 86-505.]

38. "Enterprise Projectproject": Enterprise project means an endeavor undertaken by an enterprise over a fixed period of time using information technology, which would have a significant effect on a core business function or which affects multiple government programs, agencies, or institutions. Enterprise project includes all aspects of planning, design, implementation, project management, and training relating to the endeavor. [Source: Neb. Rev. Stat. § 86-506.] Pursuant to Neb. Rev. Stat. § 86-526, the NITC is responsible for determining which proposed information technology projects are enterprise projects.

39. "Executive Managementmanagement": The means the person or persons charged with the highest level of responsibility for an Agency agency(e.g. Agency Director, CEO, Executive Board, etc.).

40. "External Networknetwork": The means the expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct Ee-commerce functions.

41. "External service provider" means a non-agency consultant, contractor, or vendor.

42. "FedRAMP" is an abbreviation for the Federal Risk and Authorization Management Program, a government wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. [http://www.fedramp.gov/]

43. "Family Educational Rights and Privacy Act (FERPA): Federal law regarding the privacy of educational information. For additional information visit the U.S. Department of Education"FERPA" is an abbreviation for the Family Educational Rights and Privacy Act, a federal act addressing the privacy of educational information.

44. "Firewall": A means a security mechanism that creates a barrier between an internal network and an external network.

45. “FTI” is an abbreviation for Federal Tax Information, and means return or return information received directly from the IRS or obtained through an authorized secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement, Bureau of the Fiscal Service, Centers for Medicare and Medicaid Services, or another entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) agreement.

46. “Geographic ~~Information~~ information ~~System~~ system”~~(GIS): A~~ means a system of computer hardware, software, and procedures designed to support the compiling, storing, retrieving, analyzing, and display of spatially referenced data for addressing planning and management problems. In addition to these technical components, a complete ~~GIS~~ geographic information system must also include a focus on people, organizations, and standards.

47. “Geospatial ~~Data~~data”~~: A term used to describe~~ means a class of data that has a geographic or spatial nature. The data will usually include locational information (latitude/longitude or other mapping coordinates) for at least some of the features within the database/dataset.

48. “GIS” is an abbreviation for geographic information system.

49. “GLBA” is an abbreviation for the Gramm-Leach-Bliley Act, a federal act requiring privacy standards and controls on personal information for financial institutions.

~~“Gramm-Leach-Bliley Act (GLB): Federal regulation requiring privacy standards and controls on personal information for financial institutions. For additional information visit the Bureau of Consumer Protection~~

50. “Guideline”~~: An~~ means an NITC document that aims to streamline a particular process. Compliance is voluntary.

51. ~~“~~Health Insurance Portability and Accountability Act ~~(HIPAA)”: A Congressional~~ is a federal act that addresses the security and privacy of health data. ~~For additional information visit Health & Human Services~~

52. “HIPAA” is an abbreviation for the federal Health Insurance Portability and Accountability Act.

53. “Host”~~: A~~ means a system or computer that contains business and/or operational software and/or data.

54. “Incident”~~: Any~~ means any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

55. “Incident ~~Response~~response”~~: An~~ means an organized approach to addressing and managing the aftermath of a security ~~breach or attack (also known as an incident)~~incident.

56. “Incident ~~Response~~ response ~~Team~~team”~~: A~~ means a group of professionals within an agency trained and chartered to respond to identified information technology incidents.

57. “Information”~~: Information is defined as~~ means the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

58. “Information ~~Assets~~assets”~~:~~ ” means (~~1~~a) All categories of automated information, including but not limited to: records, files, and databases, and (~~2~~b) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the ~~State~~state.

59. “Information ~~Security~~security”~~: The~~ means the concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss~~ (See Availability)~~.

60. “Information ~~System~~system”~~: A~~ means a system or application that consists of computer hardware, software, networking equipment, and any data. Such systems include but are not limited to desktop computers, servers, printers, telephones, network infrastructure, email, and web based services.

61. “Information ~~Technology~~technology”~~: Information technology~~ means computing and telecommunications systems and their supporting infrastructure and interconnectivity used to

acquire, transport, process, analyze, store, and disseminate information electronically. [Source: Neb. Rev. Stat. § 86-507~~.~~]

62. "Information ~~Technology~~ technology ~~Infrastructure~~infrastructure"~~: Information technology infrastructure~~ means the basic facilities, services, and installations needed for the functioning of information technology. [Source: Neb. Rev. Stat. § 86-509]

63. "Information ~~Technology~~ technology ~~Resources~~resources"~~: Hardware~~ means the hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, wide and local area networks, servers, mobile or portable computers, peripheral equipment, telephones, wireless communications, public safety radio services, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support of technology.

64. "Integrity"~~: The~~ means the assurance that information is not changed by accident or through a malicious or otherwise criminal act.

65. "Internet"~~: A~~ means a system of linked computer networks, international in scope, which facilitates data transmission and exchange, which all use the standard Internet protocol, TCP/IP, to communicate and share data with each other.

66. "Internal ~~Network~~network"~~: An~~ means an internal, ~~(i.e., non-public)~~non-public network that uses the same technology and protocols as the Internet.

67. "Internet Protocol ~~(IP)~~"~~: A~~ means a packet-based protocol for delivering data across networks.

68. "IP" is an abbreviation for Internet Protocol.

69. "IT" is an abbreviation for information technology.

70. "IT devices" means desktop computers, servers, laptop computers, personal digital assistants, MP3 players, tablet computers, mainframe computers, printers, routers, switches, hubs, portable storage devices, digital cameras, cell phones, smart phone, multi-functional

devices, and any other electronic device that creates, stores, processes, or exchanges state information.

71. "LAN" is an abbreviation for local area network.

72. "Local ~~Area~~ area ~~Network~~ network"~~(LAN): A~~ means a data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For ~~State~~ state agencies, ~~LANs~~ local area networks are defined as restricted to rooms or buildings.~~ An interconnection of LANs over a citywide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas is commonly called a wide area network (WAN).~~

73. "Malicious ~~Code~~code"~~: Malicious Code refers to~~ means code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometimes masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and computer viruses.

74. "MAC address" is an abbreviation for media access control address.

75. "MAN" is an abbreviation for metropolitan area network.

76. "MANAGED ACCESS PUBLIC" (written in all capital letters) means the data classification category defined in section 8-902.

77. "May" means that an item is truly optional.

78. "Media access control address" means a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

79. "Metropolitan ~~Area~~ area ~~Network~~ network"~~(MAN): A~~ means a data communications network that (a) covers an area larger than a local area network ~~(LAN)~~ and smaller than a wide area network~~ (WAN)~~, (b) interconnects two or more ~~LANs~~local area networks, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

80. “Must” means an absolute requirement of the specification.

81. “Must not” means an absolute prohibition of the specification.

82. “Nebraska Information Technology Commission (NITC)”: The means the information technology governing body created in Neb. Rev. Stat. § 86-515.

83. “Network Interface interface Card card”(NIC): A means a piece of computer hardware designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

84. “Network Nebraska”: The means the network created pursuant to Neb. Rev. Stat. § 86-5,100.

85. “NIC” is an abbreviation for network interface card.

86. “NIST” is an abbreviation for National Institute of Standards and Technology, a federal government entity, part of the U.S. Department of Commerce, which develops technical standards, guidelines, and frameworks.

87. “NITC” is an abbreviation for Nebraska Information Technology Commission.

88. “Not recommended” has the same meaning as should not.

89. “OCIO” is an abbreviation for Office of the Chief Information Officer.

90. “Office of the Chief Information Officer (OCIO)”: A means the division of Nebraska state government responsible for both information technology policy and operations. Statutorily, the duties previously assigned to the Division division of Communications communications and Information information Management management Services services division are part of the OCIOOffice of the Chief Information Officer.

91. “Office of the CIO” is an abbreviation for Office of the Chief Information Officer.

92. “Optional” has the same meaning as may.

93. “PCI” is an abbreviation for Payment Card Industry. The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for credit card account data protection.

94. “Personal ~~Information~~information”~~: Personal information~~ means any information concerning a person, which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

95. “Physical ~~Security~~security”~~: The~~ means the protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

96. “Policy”~~: An~~ means an NITC document that establishes a set of consistent rules and the means of achieving them that support the business objectives for the ~~State of Nebraska~~state.

97. “Principle of ~~Least~~ least ~~Privilege~~privilege”~~: A~~ means a framework that requires users be given no more access privileges ~~(read, write, delete, update, etc.)~~ to systems than necessary to perform their normal job functions, and those privileges be granted no longer than the time required to perform authorized tasks.

98. “Privacy”~~: The~~ means the right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

99. “Private ~~Information~~information”~~: Private Information~~ means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (a) social security number; ~~or~~(b) driver's license number or non-driver identification card number; or (c) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account. ~~"~~Private information~~"~~ does not include publicly available

information that is lawfully made available to the general public from federal, state, or local government records.

100. "Privileged ~~Account~~access account"~~: The~~ means the ~~User~~ user ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator~~,~~ or security administrator~~, etc~~. Special authorizations are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator~~, etc~~.

101. "Procedures"~~: Specific~~ means the specific operational steps that individuals must take to achieve goals stated in the NITC ~~Standards~~ standards and ~~Guidelines~~ guidelines documents.

102. "PUBLIC" (written in all capital letters) means the data classification category defined in section 8-902.

103. "Recommended" has the same meaning as should.

104. "Records Management Act"~~: The~~ means the Nebraska records management statutes codified at Neb. Rev. Stat. §§ 84-1201 to 84-1228.

105. "Records Officer"~~: The~~ means the agency representative ~~from the management or professional level, as appointed by each agency head,~~ who is responsible for the overall coordination of records management activities within the agency.

106. "Recovery"~~: A~~ means a defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

107. "Required" has the same meaning as must.

108. "RESTRICTED" (written in all capital letters) means the data classification category defined in section 8-902.

109. "Risk"~~: The~~ means the probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

110. “Risk ~~Assessment~~assessment”~~: The~~ means the process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

111. “Risk ~~Management~~management”~~: The~~ means the process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

112. “Router”~~: A~~ means a device or setup that finds the best route between any two networks using IP addressing, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create wide area networks.

113. “Security ~~Management~~management”~~: The~~ means the responsibility and actions required to manage the security environment including the security policies and mechanisms.

114. “Security ~~Policy~~policy”~~: The~~ means the set of criteria for the provision of security services based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

115. “Sensitive ~~Information~~information”~~: Disclosure or modification of this~~ means data, which if disclosed or modified, would be in violation of law, or could harm an individual, business, or the reputation of the agency.

116. “Sensitivity”~~: The~~ means the measurable, harmful impact resulting from disclosure, modification, or destruction of information.

117. “Separation of ~~Duties~~duties”~~: A~~ means the concept that no individual should have control over two or more phases of an operation or areas of conflicting responsibility.

118. “Shall” has the same meaning as must.

119. “Shall not” has the same meaning as must not.

120. “Should” means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighted before choosing a different course.

121. “Should not” means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighted before implementing any behavior described with this label.

122. “SISO” is an abbreviation for state information security officer.

123. “SNMP” is an abbreviation for Simple Network Management Protocol, a common protocol for network management.

124. “Staff”~~: Any~~ means ~~State of Nebraska full time and temporary~~ state employees~~, third party contractors and consultants who operate as employees, volunteers and other agency workers~~ and other persons performing work on behalf of the state.

125. “Standard”~~: Sets~~ means a set of rules for implementing policy. Standards make specific mention of technologies, methodologies, implementation procedures and other detailed factors. Adherence is required. Certain exceptions and conditions may appear in the published standard, all other deviations require prior approval.

126. “Standards and ~~Guidelines~~guidelines”~~: Refers to~~ means the collection of documents, regardless of title, adopted by the NITC pursuant to Neb. Rev. Stat. § 86-516(6) and posted on the NITC website

127. “State”~~: The~~ means the State of Nebraska.

~~State Data Communications Network (SDCN): State Data Communications Network means any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to State computers.~~

128. “State ~~Information~~ information ~~Security~~ security ~~Officer~~officer”~~: The Information Security Officer appointed by the Chief Information Officer to lead the NITC Security~~

~~Architecture Workgroup. Responsibilities include creating and maintaining polices for the State of Nebraska, conducting vulnerability / penetration tests at an enterprise level, and to assist Agency Information Security Officer's~~ means the individual employed by the state with such title.

129. "State ~~Network~~network"~~: The~~ has the same meaning as communications system ~~State of Nebraska's internal, private network, e.g. the State's 10.x.x.x address space~~.

130. "Switch"~~: A~~ means a mechanical or solid state device that opens and closes circuits, changes operating parameters or selects paths for circuits on a space or time division basis.

131. "System"~~(s): An~~ means an interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

132. "System ~~Development~~ development ~~Life~~ life ~~Cycle~~cycle"~~: A~~ means a software development process that includes defining the system requirements, the design specifications, the software development, installation and training, maintenance, and disposal.

133. "TCP/IP"~~: An~~ is an abbreviation for Transmission Control Protocol / Internet Protocol. A protocol for communications between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

134. "Technical ~~Panel~~panel"~~: The~~ means the panel created in Neb. Rev. Stat. § 86-521.

~~Third Party: Any non-agency contractor, vendor, consultant, or external entity, etc.~~

135. "Threat"~~: A~~ means a force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

136. "Token"~~: A~~ means a device that operates much like a smart card but is in a physical shape that makes its use easier to manage.

137. "Trojan ~~Horse~~horse"~~: Illegal~~ means code hidden in a legitimate program that when executed performs some unauthorized activity or function.

138. “UID” is an abbreviation for user ID.

139. “Unauthorized ~~Access~~ access ~~Or~~ or ~~Privileges~~privileges”~~: Insider or outsider who gains~~ means access to network or computer resources without permission.

140. ~~“~~User”:~~ Any agency (ies), federal government entity (ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose~~ means a person who is authorized to use an information technology resource.

141. “User ID” is an abbreviation for user identifier, and means a system value, when associated with other access control criteria, used to determine which system resources a user can access.

142. “Virtual ~~Local~~ local ~~Area~~ area ~~Network~~ network”~~(VLAN): A VLAN is~~ means a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.

143. “Virtual ~~Private~~ private ~~Network~~ network”~~(VPN): A~~ means a communications network tunneled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. A VPN may have best-effort performance, or may have a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point. The distinguishing characteristic of VPNs are not security or performance, but that they overlay other network(s) to provide a certain functionality that is meaningful to a user community.

144. “Virus”~~: A~~ means a program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

145. “VLAN” is an abbreviation from virtual local area network.

146. “VPN” is an abbreviation for virtual private network.

147. “Vulnerability”~~: A~~ means a weakness of a system or facility holding information that can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

148. “Vulnerability ~~Scanning~~scanning”~~: The~~ means the portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

149. “Web ~~Application~~application”~~: An~~ means an application that is accessed with a web browser over a network such as the Internet or an intranet.

150. “Web ~~Page~~page”~~: A~~ means a document stored on a server, consisting of an HTML file and any related files for scripts and graphics, viewable through a web browser on the World Wide Web. Files linked from a ~~Web~~ web ~~Page~~ page such as Word (.doc), Portable Document Format (.pdf), and Excel (.xls) files are not ~~Web~~ web ~~Pages~~pages, as they can be viewed without access to a web browser.

151. “Web ~~Site~~ site or ~~Website~~website”~~: A~~ means a set of interconnected ~~Web~~ web ~~Pages~~pages, usually including a homepage, generally located on the same server, and prepared and maintained as a collection of information by a person, group, or organization.

152. “Wide ~~Area~~ area ~~Network~~ network”~~(WAN): A~~ means a physical or logical network that provides data communications to a larger number of independent users than are usually served

by a local area network ~~(LAN)~~ and is usually spread over a larger geographic area ~~than that of a LAN~~.

153. "Wireless ~~Local~~ local ~~Area~~ area ~~Network~~ network"~~(WLAN): A wireless local area network (or wireless LAN, or WLAN) is~~ means the linking of two or more computers without using wires. ~~WLAN~~ A wireless local area network utilizes technology based on radio waves to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network.

154. "WAN" is an abbreviation for wide area network.

155. "WLAN" is an abbreviation for wireless local area network.

156. "Worm"~~: A~~ means a program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

Sec.2. Original section 1-101 is repealed.

Sec.3. Subsections 23, 76, 102 and 108 of section 1 of this proposal become operative on December 1, 2017. The other provisions of this proposal take effect when approved by the Commission.

State of Nebraska
Nebraska Information Technology Commission
Technical Standards and Guidelines

Proposal 17-01
Final

A PROPOSED NEW POLICY relating to information security.

Section 1. The following provisions constitute a new CHAPTER 8 of the Technical Standards and Guidelines:

CHAPTER 8

INFORMATION SECURITY POLICY

Article.

1. Purpose; Scope; Roles and Responsibilities; Enforcement and Policy Exception Process.
2. General Provisions.
3. Access Control.
4. Network Security.
5. System Security.
6. Application Security.
7. Auditing and Compliance.
8. Vulnerability and Incident Management.
9. Data Security.

ARTICLE 1

PURPOSE; SCOPE; ROLES AND RESPONSIBILITIES; ENFORCEMENT AND POLICY EXCEPTION PROCESS

8-101. Purpose

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. This Information Security Policy contains the safeguards, responsibilities and acceptable behaviors required to establish and maintain a secure environment.

8-102. Scope

This policy is applicable to state agencies, boards, and commissions, excluding higher education entities. This policy applies to all information technology systems for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of an agency. In the event an agency has developed policies or additional requirements for information security, the more restrictive policy will apply.

8-103. Roles and Responsibilities

State Agencies

Agencies that create, use, or maintain information systems for the state must create and maintain an information security program consistent with this policy to ensure the confidentiality, availability, and integrity of the state's information assets.

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.

State Information Security Officer

The state information security officer performs as a security consultant to agencies and agency information security officers to assist the agencies in meeting the requirements of this policy. The state information security officer may also perform periodic reviews of agency security for compliance with this and other security policies and standards.

Agency 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 for

their agency. 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

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

Technical Panel

The technical panel is responsible for recommending technical standards and guidelines to be considered for adoption by the Nebraska Information Technology Commission.

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.

Security Architecture Workgroup

The security architecture workgroup is a workgroup 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 security issues; document existing problems, potential points of vulnerability, and related risks; and, determine security requirements of state agencies stemming from state and federal laws or regulations.

8-104. Enforcement and Policy Exception Process

This policy establishes the controls and activities necessary to appropriately protect information and information technology resources. While every exception to a policy or standard weakens the protection for state IT resources and underlying data, it is recognized that at times business requirements dictate a need for temporary policy exceptions. In the event an agency believes it needs an exception to this policy, the agency may request an exemption by following the procedure outlined in section 1-103.

ARTICLE 2

GENERAL PROVISIONS

8-201. Acceptable Use

Subject to additional requirements contained in state law, the following are the policies and provisions governing the acceptable use of information technology resources in state government:

(1) NITC 7-101 is the acceptable use policy for the state network;
(2) Neb. Rev. Stat. § 49-14,101.01 establishes certain statutorily prohibited uses of public resources; and
(3) the following acceptable use provisions are established by this policy:
   (a) all state electronic business must be conducted on approved IT devices;
   (b) accessing or attempting to access CONFIDENTIAL or RESTRICTED information for other than a required business "need to know" is prohibited; and
   (c) Misrepresenting yourself as another individual or organization is prohibited.

Use of state information technology resources may be monitored to verify compliance with this policy.

8-202. Change Control Management

To protect information systems and services, a formal change management system must be established to enforce strict controls over changes to all information processing facilities, systems, software, or procedures. Agency management must formally authorize all changes before implementation and ensure that accurate documentation is maintained.

The change management process may differ between changes to IT infrastructure (which includes all hardware, system software, and network assets) and application software (which includes commercial off the shelf data applications and in-house developed data application software). However, underlying requirements for managing change are the same. All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release and does not unknowingly add security risks to the state's environment. All changes to network perimeter protection devices should be included in the scope of change management.

IT Infrastructure - The following change management standards are required to be followed for all IT infrastructure.

1. The Office of the CIO requires a change management process with assigned responsibilities to ensure all changes to hardware, system software, and network infrastructure are authorized. This process will include representation from the Office of the CIO, agency, state information security officer, and application development (when application changes impact or are impacted). This process must occur on a periodic basis with sufficient frequency to meet demands for changes to the environment.

2. All records, meetings, decisions, and rationale of the change control group must be documented and securely stored for audit purposes. The agenda for this meeting is flexible but should generally address a review of at least the following:

   A. Change summary, justification and timeline;

B. Functionality, regression, integrity, and security test plans and results;

C. Security review and impact analysis;

D. Documentation and baseline updates; and

E. Implementation timeline and recovery plans.

3. The agency is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as CONFIDENTIAL information, and secured appropriately. The baseline documents must be reviewed and updated on an annual basis or after any significant changes to the baseline have been installed.

4. All changes to the production infrastructure are required to be made by authorized personnel only, using access credentials assigned to that individual. Actions performed by these user credentials will be logged.

Application Development – The following change management standards are required to be followed for application software systems that create, process, or store CONFIDENTIAL or RESTRICTED data.

1. Application change management processes must be performed with assigned responsibilities to ensure all changes to application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements.

2. The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request.

3. The change management processes will retain a documented history of the change process as it passes through the software development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following:

    A. Change summary, justification, and timeline;

    B. Functionality, regression, customer acceptance, and security test plans;

    C. Security review and impact analysis;

    D. Documentation and baseline updates; and

    E. Implementation timeline and recovery plans.

4. Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must be implemented.

5. Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place that ensure the confidentiality, integrity, and availability of the data maintained in the production library.

6. Application development changes that impact IT infrastructure must be submitted to the infrastructure change management process for review, approval, and implementation coordination.

8-203. Multi-Function Devices

All multi-function devices used to process, store, or transmit data must be approved by the state information security officer or agency information security officer. The device must be configured and managed to adequately protect sensitive information.

Configuration and management of multi-function devices must include minimum necessary access to the processing, storing, or transmitting functions. All unnecessary network protocols and services must be disabled. Access controls must be in place, and administrator privileges must be controlled and monitored. Auditing and logging must be enabled. Access to the internal storage must be physically controlled. The devices must be securely disposed or cleansed when no longer needed. Software and firmware must be updated to the latest version supported by the vendor. All CONFIDENTIAL or RESTRICTED information must be encrypted in transit when moving across a WAN as well as when stored on the internal storage unit of the device. If the device stores information and is not capable of encrypting internal storage, then it must be physically secured or not used for CONFIDENTIAL or RESTRICTED information. Encryption technology must be approved by the state information security officer or agency information security officer.

8-204. Email

Users of the state email system must not set up rules, or use any other methodology, to automatically forward emails to a personal or other account outside of the state network unless approved by the state information security officer or the agency information security officer.

CONFIDENTIAL or RESTRICTED data must not be sent by email unless it has been encrypted using technology approved by the state information security officer or the agency information security officer.

8-205. Portable IT Devices

CONFIDENTIAL or RESTRICED data must not be stored on portable IT devices unless it has been encrypted using technology approved by the state information security officer or the agency information security officer.

8-206. Facilities; Physical Security Requirements

Agencies must perform a periodic threat and risk assessment to determine the security risks to facilities that contain state information, and implement reasonable and appropriate physical security measures to prevent and detect unauthorized access, theft, damage or interference.

Based on the threat and risk assessment, a multi-layered physical security perimeter must be established in agency environments where information or information assets are stored or where operational data centers, network wiring closets, or telephony connection equipment exists, or where printers that print CONFIDENTIAL or RESTRICTED information are used, and any other location where information may be in use or stored, such as file cabinets, microfiche storage areas, etc. The security layers create a perimeter that would require multiple methods of access control to gain entry. These layers could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office, or another physical barrier. CONFIDENTIAL or RESTRICTED information must maintain at least two barriers to access at all times.

8-206. Facilities; Identification Badges and Visitors

Only authorized individuals are allowed to enter secure areas of state facilities that contain information technology infrastructure. Those individuals will be issued an electronic ID badge. All authorized individuals are required to scan their ID badge before entry into these secure areas. ID badges must be visible, and staff are encouraged to question anyone they do not recognize who is not wearing a badge. Staff who forget their badges will be issued a temporary badge after management approval. Temporary badges must be returned at the end of the day.

All visitors are required to sign a visitor's log, including the following information: name, organization, signature, purpose of visit, date, time in, time out, and person to see. Visitors will be assigned a temporary badge that must be visible at all times. Visitors are not allowed into secure areas such as data centers. If it is necessary for a visitor to enter a secure area, they must be escorted at all times. When exiting the facility, the visitor must sign out and return the badge while under staff supervision.

8-207. State and 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:

1. Information security strategic plan;
2. System security plan(s); and
3. Plan of actions and milestones (POA&M).

These reports will reflect the current and planned state of information security at the agency.

A. <u>Information Security Strategic Plan</u>

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 be updated and published on an annual basis, and should include a 5-year projection of key security business drivers, 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.

<u>Contents of the Information Security Strategic Plan:</u>

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.
8. Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect information security.
9. Proposed five-year timeline of events and key deliverables or milestones.
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.
    d. Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

B. <u>System Security Plan</u>

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 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 develop or update the SSP in response to each of the following events:

- New system
- Major system modification

- Increase in security risks / exposure
- Increase of overall system security level
- Serious security violation(s)
- 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 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. 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. Review of security controls and assessment results that have been conducted within the past three years.
11. 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.

C. Plan of Action and Milestones Report (POA&M)

The POA&M is a reporting tool that outlines weaknesses and delineates the tasks necessary to mitigate them. The information security POA&M process will be used to facilitate the remediation of information security and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions
- Defining roles, responsibilities, and accountabilities for weakness resolution
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources
- Ensuring appropriate progress and priorities are continually addressed
- Informing decision makers

The POA&M process provides significant benefits to the state. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, a POA&M must be continually monitored and diligently updated. The state information security officer and agency information security officers are responsible for maintaining the POA&M and for providing quarterly updates to the leadership.

Contents of the Information Security Plan of Action with Milestones:

1. Source – Identifies the audit, review, event or procedure which identified this action item
2. ID – Identification tracking number of this action item which can be tied to the source and timeframe of identification
3. Project/Task – Defines the project, task objective and goals of the action item
4. Key content and description – Narrative describing the key elements of the action item
5. Key milestones – Lists each measurable activity required to complete the action item
6. Milestone status – Lists the status of each milestone (Open, Completed, Closed Assigned, In Progress)
7. Target or completion date – Expected date each milestone will be completed. The agency should also accommodate approved changes to target dates in a manner that reflects the new date while keeping record of the original due date.
8. Responsible party – List of individuals or support unit assigned to address the action item

ARTICLE 3

ACCESS CONTROL

8-301. Remote Access Standard

It is the responsibility of all agencies to strictly control remote access from any device that connects from outside of the state network to a desktop, server or network device inside the state network and ensure that employees, contractors, vendors and any other agent granted remote access privileges to any state network utilize only approved secure remote access tools and procedures.

The following standards apply to all staff that connect to the state network through the Internet. This includes all approved work-from-home arrangements requiring access to state systems and agency office locations that use the Internet to access the state network. Each state agency will be responsible for ensuring that remote access to state resources is secured and compliant with this policy.

(1) The following are the general requirements for remote access:
   (a) Requests for remote access must be reviewed and approved by the state information security officer and the agency information security officer prior to access being granted.
   (b) Staff approved for remote connectivity are required to comply with all policies and standards.
   (c) All devices connecting to the network must have up-to-date anti-virus protection, active firewalls, and appropriate security patch levels equivalent to those provided for state equipment.
   (d) All remote access sessions must be logged. The Office of the CIO or the agency will perform periodic monitoring of remote access sessions with random inspections of the user security settings and protocols to ensure compliance with this policy.
   (e) Remote access logon failures must be logged. Credentials must be disabled after three (3) consecutive failed login attempts.
   (f) Remote sessions must be locked after no more than 15 minutes of inactivity until the user re-establishes access with the appropriate credentials and authentication procedures.
   (g) Staff with remote access privileges must ensure that their computer which is remotely connected to the state network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

(2) The following are additional requirements for remote access to data classified as CONFIDENTIAL or RESTRICTED:
   (a) Requests for remoted access must indicate if CONFIDENTIAL or RESTICTED data may be accessed.
   (b) Mechanisms must be employed to ensure personally identifiable information, or other sensitive information cannot be downloaded or remotely stored.

(c) All state owned or managed devices must be password protected and full-disk encrypted using approved technology. Encryption technology must be provided or approved by the Office of the CIO.

(d) Remote sessions that store, process, or access CONFIDENTIAL or RESTRICTED information or systems must use access control credentials and an approved form of multi-factor authentication before connecting to the state network. Remote sessions must employ Office of the CIO approved cryptography during the entire session when connected to the state network.

8-302. Minimum Password Configuration

A. Minimum Password Requirements

The following are the minimum password requirements for state government passwords:

- Must contain a minimum Eight (8) characters
- Must contain at least Three (3) of the following Four (4):
- At least One (1) uppercase character
- At least One (1) lowercase character
- At least One (1) numeric character
- At least One (1) symbol (!@#$%^&)
- Cannot repeat any of the passwords used during the previous 365 days.

In addition to the minimum password complexity outlined above, additional password requirements are necessary for differing levels of data classification when authenticating users to networks or applications. The highest data classification level that a user has access to during an authenticated session will determine the additional password requirements. All employees and contractors of the state shall use a password that follows at least a confidential level of authentication when logging into a state network or application.

B. Additional Access Requirements for RESTRICTED Information

Information that is classified as RESTRICTED requires the highest level of security. This includes root/admin level system information accessed by privileged accounts. A password used to access RESTRICTED information must follow the password complexity rules outlined in subsection A, and must contain the following additional requirements:

- Multi-factor authentication
- Expire after 60 days
- Minimum Password Age set to 15 days
- Accounts will automatically be disabled after three unsuccessful password attempts

C. Additional Access Requirements for CONFIDENTIAL Information

Information that is classified as CONFIDENTIAL requires a high level of security. A password used to access CONFIDENTIAL information must follow the password complexity rules outlined in subsection A, and must contain the following additional requirements:

- Expire after 90 days
- Accounts will automatically lock after three consecutive unsuccessful password attempts

D. Password Requirements for MANAGED ACCESS PUBLIC Information

Information that is classified as MANAGED ACCESS PUBLIC requires minimal level of security and need not comply with subsection A. Typically, this data would not include personal information but may carry special regulations related to its use or dissemination. MANAGED ACCESS PUBLIC data may also be data that is sold as a product or service to users that have subscribed to a service.

E. Password Requirements for Accessing PUBLIC Information

Information that is classified as PUBLIC requires no additional password security and need not comply with subsection A.

F. Non-Expiring Passwords

Non-expiring passwords require a unique high level of security. Typically this information is confidential in nature and must follow the requirements in subsection A. The additional requirements for access to CONFIDENTIAL or RESTICTED data with a non-expiring password are:

- Extended password length to 10 characters
- Independent remote identity proofing may be required
- Personal security question may be asked
- Multi-factor authentication
- Any feature not included on this list may also be utilized upon approval of the state information security officer.

G. Automated System Accounts

Examples of automated system accounts include those that act as an intermediary between the public user and state systems, internal system to system interfaces, perform backups or run batch jobs. System account passwords shall expire after 365 days, unless mechanisms to restrict the use of those credentials to just the authorized service can be implemented and approval is granted by the state information security officer.

H. Multi-user Computers

Multi-user computers include those computers in kiosks or training labs, where users have limited or restricted access to state resources. Agencies may use non-expiring passwords on multi-user computers. In these cases, mechanisms to ensure the user account with non-expiring passwords is unable to access CONFIDENTIAL or RESTRICTED information.

I. System Equipment/Devices

Agencies may use non-expiring passwords for system equipment/devices. It is common for many devices (e.g., IP cameras, HVAC controls) in today's IT environment to utilize login capabilities to protect the device from unauthorized access. While many of these devices make use of a user ID

and password in a manner like those found while authenticating a user, the distinction to be made is that the user ID is used to authenticate the device itself to the system and not a person.

8-303. Identification and Authorization

A. All employees and other persons performing work on behalf of the state, authorized to access any state information or IT resources, that have the potential to process, store, or access non-public information, must be assigned a unique State of Nebraska user ID which resides in the State of Nebraska Active Directory domain with the minimum necessary access required to perform their duties.

B. Staff are required to secure their user IDs from unauthorized use.

C. Sharing user IDs is prohibited.

D. To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical. Whenever separation of duties is impractical, other compensatory controls such as monitoring of activities, increased auditing and management supervision must be implemented. At a minimum, the audit of security must remain independent and segregated from the security function.

8-304. Privilege Access Accounts

Privileged access accounts include administrator accounts, embedded accounts used by one system to connect to another, and accounts used to run service programs. These accounts are used by systems and personnel to access sensitive files, execute software, load and configure policies and configuration settings, and set up or maintain accounts.

Due to the elevated access levels these accounts typically have, the following standards and procedures must be followed to minimize the risk of incidents caused by these accounts:

- All privileged access accounts must be assigned to an individual with an approved business need for the privileged access. These accounts must not be shared.
- Default administrator accounts must be renamed, removed or disabled. Default passwords for renamed or disabled default administrator accounts must be changed.
- Default system account credentials for hardware and software must be either disabled, or the password must be changed. Use of anonymous accounts is prohibited, and unassigned accounts must be assigned to an individual prior to use. When no longer needed, the account must be disabled. At all times, the state requires individual accountability for use of privilege accounts.
- Privileged access accounts will have enhanced activity logging enabled. The Office of the CIO and all applicable agencies will perform a quarterly review of privileged access account activity.
- Privileged access through remote channels will be allowed for authorized purposes only and must include multi-factor authentication.
- Passwords for these accounts must be changed every 60 days.

- The password change process must support recovery of managed systems from backup media. Historical passwords should remain accessible in a history table in the event that they are needed to activate a backup copy of a system.
- Privileged access accounts must be approved, provisioned, and maintained by the Office of the CIO.

ARTICLE 4

NETWORK SECURITY

8-401. Network Documentation

The State of Nebraska encourages the use of its electronic communications infrastructure in support of its mission. However, this infrastructure must be well-managed and protected to ensure the security of Agency information. Therefore, all network devices that access the state internal network are required to adhere to these standards.

The Office of the CIO and agencies will implement a range of network controls to ensure the confidentiality, integrity, and availability of the data flowing across its trusted, internal network, and ensure the protection of connected services and networks. The Office of the CIO ensures that measures are in place to mitigate security risks created by connecting the state network to a third party network. All direct connections to the state network and direct connections between agencies must be authorized by the Office of the CIO.

Where an agency has outsourced a server or application to an external service provider (such as a web application), the agency must perform or have performed a security review of the outsourced environment to ensure the confidentiality, integrity, and availability of the state's information and application is maintained. For applications hosted by Nebraska.gov, the Nebraska State Records Board will perform the security review on behalf of all agencies.

All publicly accessible devices attached to the state network must be registered and documented in the IT Inventory system. Additions or changes to network configurations, including through the use of external service providers, must be reviewed and approved through the Office of the CIO's change management process.Publicly accessible devices must reside in the Office of the CIO's DMZ unless approved by the Office of the CIO for legitimate business purposes.

8-402. Network Transmission Security

1 All encryption must be approved by the state information security officer. Any transmissions over unsecured networks (such as the Internet) that contain CONFIDENTIAL or RESTRICTED information must be encrypted using technology that is FIPS 140-2 compliant.

2 Network scanning and monitoring is prohibited, unless prior approval is obtained from the Office of the CIO. If approved, scanning must be restricted to authorized and registered IP addresses only, and conducted by authorized personnel only.

3 The Office of the CIO shall ensure that all networks and systems are monitored 24x7 with authorized tools (such as network based intrusion detection and prevention systems) and personnel to detect system anomalies or security events.

4 Passwords and SNMP community names may not be sent in clear text over open networks. All devices must use authorized encryption for access authorization to the state network. Access to the DMZ applications is exempt from this requirement.

8-403. Network Architecture Requirements

1 All devices that store, access, or process CONFIDENTIAL or RESTRICTED information must not reside in the public tier, and must be protected by at least two firewalls. Firewalls must be placed at perimeter locations so that all critical systems are protected by multiple firewalls and monitoring systems.

2 All publicly accessible devices must be located in an access-controlled environment, and access credentials must be managed by authorized personnel.

3 All network devices that contain or process CONFIDENTIAL or RESTRICTED data must be secured with a password-protected screen saver that automatically locks the session after no more than 15 minutes of inactivity.

4 Devices that include native host-based firewall software in the operating system must have the firewall activated and properly configured, unless the active firewall software compromises the usability of critical applications, or lessens the posture of other security systems.

5 The state network will have an annual verification of all open ports, protocols, and services for publicly accessible systems.

6 Any requests for public IP addresses or for additional open ports must be approved by the state information security officer.

7 Staff will follow approved change control and configuration management procedures for network devices. Patches and hot-fixes recommended by network hardware or software vendors must be installed as soon as practical after testing.

8 Services and applications that will not be used must be disabled or removed if such action will not negatively impact operations. Protocols such as telnet, VNC, RDP, or others that do not actively support approved encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

8-404. External Connections

Direct connections between the state network and external networks must be implemented in accordance with these policies and standards. Connections will be allowed only when external networks have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented to protect state resources. A risk analysis should be performed to ensure that the connection to the external network would not compromise the state network. Additional controls, such as the establishment of firewalls and a DMZ may be implemented between any third party and the state. All external connections will be reviewed on an annual basis.

External network and workstation connections to the state network must have an agency sponsor and a business need for the network connection. The external network equipment must also conform to the state's security policies and standards, and be approved by the Office of the CIO.

Any connection between agency firewalls over public networks that involves sensitive information must use encryption to ensure the confidentiality and integrity of the data passing over the external network.

8-405. Wireless Networks

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However, security risks, if not addressed correctly, could expose state information systems to a loss of service or compromise of sensitive information. Everything transmitted over radio waves (wireless devices) can be intercepted. This represents a potential security issue. Agencies shall take appropriate steps, including the implementation of encryption, user authentication, and virus protection measures, to mitigate risks to the security of state data and information systems associated with the use of wireless network access technologies.

No wireless network or wireless access point will be installed without the written approval of the Office of the CIO.

All wireless networks will be inspected annually by the state information security officer and agency information security officer to ensure proper security protocols are in place and operational.

ARTICLE 5

SYSTEM SECURITY

8-501. System Documentation

1. Only Office of the CIO approved hardware or software is permitted within the state's information technology infrastructure.
2. All authorized hardware and software shall be inventoried and documented. Results shall be secured in an auditable fashion.

8-502. Minimum User Account Configuration

User accounts must be provisioned with the minimum necessary access required to perform duties. Accounts must not be shared, and users must guard their credentials.

Administrator level access is privileged and must be restricted to authorized IT personnel only. All privileged access accounts are subject to additional security, including multi-factor authentication, and enhanced auditing and logging of activity.

Local accounts must be disabled unless required for business purposes, and in those cases, use of these accounts must be approved, tightly controlled, and monitored. All use of local accounts are required to be associated with an individual user.

8-503. Minimum Server Configuration and Patch Management

The state recognizes the National Institute of Standards and Technology (NIST) as a source for recommended security requirements that provide minimum baselines of security for servers.

NIST provides instructions, recommendations, and considerations to assist readers in deploying servers in a secure method. All state system administrators should examine NIST 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 NIST standards, guidelines, and checklists as identified below.

- NIST 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-70, The NIST Security Configuration Checklists Program
- NIST SP 800-44, Guidelines on Securing Public Web Servers

Server Hardening

All 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.

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 personnel only, and all vendor supplied patches must be applied. All software and hardware components should be currently supported. All unsupported hardware and software components must be identified and have a management plan that is approved by the state information security officer.
3. All unnecessary software, system services, accounts and drivers must be removed unless doing so would have a negative impact on the server.
4. Logging of auditable events, as defined in NIST 800-53 control objectives, will be enabled. Audit logs will be secured and only accessible to accounts with privileged access.
5. Security parameters and file protection settings must be established, reviewed, and approved by the state information security officer.
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 Department and as referenced in the National Vulnerability Database (HTTP://nvd.nist.gov).
7. Hardened servers will be scanned monthly for unauthorized software or unauthorized changes to the configuration baselines.
8. Hardened servers will be monitored with active intrusion detection, intrusion protection, or 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 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.
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 should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.

8-504. Minimum Workstation Configuration

Improperly configured workstations are at risk to be compromised. Without proper adherence to these workstation security standards, the state is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect the state from unauthorized data or activity residing or occurring on state equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout the state networks or launching other

attacks. All managed workstations that connect to the state's network are required to meet these standards. The Office of the CIO is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. Workstation standards should be securely maintained and stored in a centralized documentation library. In addition to adherence to the required images, the following standards are defined for all workstations that connect to the state network. The degree of protection of the workstation should be commensurate with the data classification of the resources stored, accessed, or processed from this computer.

1. Endpoint security (anti-virus) software, approved by the Office of the CIO, must be installed and enabled.
2. The host-based firewall must be enabled if the workstation is removed from the state network.
3. The operating system must be configured to receive automated updates.
4. The system must be configured to enforce password complexity standards on accounts.
5. Application software should only be installed if there is an expectation that it will be used for state business purposes. Application software not in use should be uninstalled.
6. All application software must have security updates applied as defined by patch management standards.
7. Web browsers settings should be selected or disabled as appropriate to increase security and limit vulnerability to intrusion.
8. Shared login accounts are prohibited unless approved in advance and configured by IT. Shared login accounts are only acceptable if approved through the policy exception process and alternate mechanisms or access layers exist to ensure the ability to individually identify personnel accessing non-public information.
9. Shared login accounts are forbidden on multi-user systems where the manipulation and storage of CONFIDENTIAL or RESTRICTED information takes place.
10. Users need to lock their desktops when not in use. The system must automatically lock a workstation after 5 minutes of inactivity.
11. Users are required to store all CONFIDENTIAL or RESTRICTED information on IT managed servers, and not the local hard drive of the computer. Local storage may only be used for temporary purposes when the data stored is not sensitive, and where loss of the information will not have any detrimental impact on the state.
12. All workstations shall be re-imaged with standard load images prior to re-assignment.
13. Equipment scheduled for disposal or recycling must be cleansed following agency media disposal guidelines

8-505. Minimum Laptop Configuration

In addition to the requirements contained in section 8-504, all laptops that connect to the state network are required to meet the following requirements.

1. Remote access to CONFIDENTIAL or RESTRICTED information must occur through a state-managed endpoint, using the state VPN or other connections that have been approved by the Office of the CIO.
2. Remote access to any privilege functions, such as administrator accounts, must employ multi-factor authentication and all activity must be logged for audit purposes.
3. Remote access users are responsible for all actions incurred during their session in accordance with all state and agency standards and policies.
4. All home networks connected to the Internet via a broadband connection should have a firewall installed, updated and operational.
5. Laptops with remote access to, or the capability to store, CONFIDENTIAL or RESTRICTED data are required to be fully encrypted using technology approved by the state information security officer.

8-506. Minimum Mobile Device Configuration

All mobile computing devices accessing the state network or containing state information must be provisioned to meet these security policies and be approved by the Office of the CIO. All devices that will be connected to the state network must be logged with device type and approval date.

1. Mobile computing devices must be shut down or locked when not in use. These devices must not be left unattended in a public access area. They must be locked in a secure cabinet or room, or kept on the person. Devices should not be shared.
2. Mobile computing devices and mobile storage devices must not be left in a vehicle unattended.
3. Storing CONFIDENTIAL or RESTRICTED information on any mobile device or any removable or portable media (e.g., CDs, thumb drives, DVDs) is prohibited unless arrangements and mechanisms for securing the data has been explicitly approved by the state information security officer. In those cases, all mobile computing devices or portable media shall be encrypted using technology that is approved by the state information security officer.
4. Personally owned mobile devices (e.g., smartphones and tablets) may be used for approved state purposes, including email, when configured to access the state information through a managed interface or sandbox only. Devices that are not configured to use the authorized interface are prohibited from accessing any state information, including email.
5. The device must have security settings that block users from changing mandatory settings.
6. Strong passwords are required, and passwords must change regularly per state policy regarding passwords.
7. The device must lock after no more than 5 minutes of inactivity and must require the re-entry of a password or PIN code to unlock.

8. After 10 unsuccessful password attempts, the device or the state container will be erased. In the event that the device becomes lost or stolen, the Office of the CIO must have the capability to remotely locate, lock, and erase the device.
9. The device should have all data backed up at the state data center.
10. Devices need to be cleared of all information from the prior user before being issued to a new user.
11. The device OS must be up to date and patched. New versions of the OS must be vetted for security posture and supportability.
12. Devices must be properly disposed of using mechanisms approved by the state information security officer. State data must be cleared and devices properly disposed of or recycled. The disposition process is required to be documented and periodically audited.
13. New devices are required to be configured and operate within established security guidelines and help desk support must be established before these devices can be operational. New devices need to be validated before being made available for users to request.

8-507. System Maintenance

1. All systems involved in the processing, storage, or access to any CONFIDENTIAL or RESTRICTED information must be maintained per manufacturer specifications. Maintenance personnel must be approved for this activity by the state information security officer and must be briefed on the requirements for protecting sensitive information.
2. Maintenance activity must be logged to include the date/time of the maintenance, activity performed, the person or organization who performed the maintenance, the name and department of the escort (if applicable), and a detailed list of any equipment removed or replaced during the maintenance. This list should include serial numbers, if applicable.
3. Prior to removing any equipment from the secured environment to which it is assigned, the equipment must be approved for release and validated by the state information security officer that all non-public information has been encrypted, secured, or permanently deleted from the equipment. When equipment is returned, it must be inspected for unauthorized systems, settings, or services to ensure the integrity of the security systems before reloading data or placing back into the environment.
4. All tools used for maintenance must be tested. The Office of the CIO must maintain a list of approved maintenance tools that is reviewed and updated at least annually.
5. Nonlocal or remote maintenance must be approved in advance by the state information security officer or the Office of the CIO, and must also comply with all agency and Office of the CIO requirements for remote access.
6. All remote maintenance activity must be logged and reviewed.
7. Maintenance of agency-developed software must follow the state's change management process to ensure changes are authorized, tested and accepted by agency management. All known security patches must be reviewed, evaluated and appropriately prioritized.

8. Critical patches must be applied within 24 hours of receipt. High risk patches must be applied within 7 days of receipt. All other patches must be appropriately applied in a timely manner as determined by the agency.
9. All vendor supplied software deployed and operational must be currently supported by the vendor.

ARTICLE 6

APPLICATION SECURITY

8-601. Application Documentation

To ensure that security is built into applications, security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to, and documented as part of the overall business case for the system. To ensure this activity is performed, the agency information security officer must be involved in all phases of the application development life cycle from the requirements definition phase, through implementation and eventual application retirement.

Controls in applications may be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, and included in the agency's security standards documents. The security measures that are implemented must be based on the threat, vulnerability, and risk assessments of the information being processed and cost-benefit analysis.

Significant changes involving applications that store, access, or process CONFIDENTIAL or RESTRICTED information must go through a formal change management process. For recurring maintenance of these applications, an abbreviated change management process may suffice if that abbreviated process has been approved by the state information security officer.

8-602. Application Code

Access to source code libraries for both agency business applications and operating systems must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

All application source code must be backed up and access restricted to authorized personnel only. Application changes are required to go through a software development life cycle process that ensures the confidentiality of information, and integrity and availability of source and executable code. Application changes must follow the change management process as defined in section 8-202.

8-603. Separation of Test and Production Environments

Development software and testing tools can cause serious problems to the production environment if separation of these environments does not exist. Separation of the development, test and production environments is required, either on physically separate machines or separated by access controlled domains or directories. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. Each agency must consider the use of a quality assurance environment where user acceptance testing can be conducted. The following controls must be considered:

- Access to compilers, editors and other system utilities must be removed from production systems when not required.

- Logon procedures and environmental identification must be sufficiently unique for production testing and development.
- Access to systems and business applications must be restricted to those individuals who have a business need to access those resources in the performance of their job responsibilities.
- It is recognized that at times, business or technical requirements dictate the need to test with live data. In those cases, it is mandatory to have approval from the state information security officer, and to implement production-class controls in the applicable test environment to protect that information.

8-604. Application Development

The following standards are required to be followed for agency developed application software that create, process, or store CONFIDENTIAL or RESTRICTED data.

1. The agency must establish an application change management processes with assigned responsibilities to ensure all changes to applicable application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent state information security requirements.
2. The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request.
3. The change management processes must retain a documented history of the change process as it passes through the application development life cycle with documentation securely stored for audit purposes. Documentation should address a review of the following:
    a. Change summary, justification, and timeline
    b. Functionality, regression, integrity, and security test plans and results
    c. Security review and impact analysis
    d. Documentation and baseline updates
    e. Implementation timeline and recovery plans
4. Changes to software applications must be controlled and production installations must be made by personnel assigned to update production libraries. Mechanisms to maintain and ensure the integrity of the application code must be implemented.
5. Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place which ensure the confidentiality, integrity, and availability of the data maintained in the production library.
6. Application development changes that impact agency IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation
7. The security requirements of new applications must be established, documented and tested prior to their acceptance and use. The agency information security officer must ensure that acceptance criteria are utilized for new applications and upgrades. Acceptance testing must be performed to ensure security requirements are met prior to the application being migrated to the production environment.

8. All applications are required to maintain up-to-date documentation that includes an assessment of security threats and impacts, and a detailed description of the data handling with its accurate classification.
9. Applications that provide user interfaces must have an appropriate warning banner displayed, applicable to the data being accessed (e.g., PHI, FTI, PII).
10. Application credentials, where possible, should be inherited from the state managed authentication source. If that is not possible, credentials should have the same level of management and approval as other agency access credentials.
11. Applications must be configured such that CONFIDENTIAL or RESTRICTED data will be encrypted when transmitted outside the agency internal network.

8-605. Security Standards for Web Applications and Services

Internet-facing systems are diverse to meet a multitude of different needs. Therefore, information exposures by these systems differ, as do threats. Security controls should be implemented to mitigate meaningful risks to an application. Because every system is different, the web application developer is the most knowledgeable about the system and the risks it faces.

This standard establishes a baseline of security requirements for all state websites, web services, and all vendor supported or hosted web applications. All applications that are Internet-facing are required to securely maintain documentation and evidence of compliance levels with this standard.

This standard is based on the research and recommendations from the SysAdmin, Audit, Network, and Security (SANS) Institute and the Open Web Application Security Project (OWASP).

1. Consider the threats, vulnerabilities, and risks to your application. If you are unsure, follow the threat risk methodology published by OWASP.

   http://www.owasp.org/index.php/Threat_Risk_Modeling
2. Consider and implement additional security controls to ensure the confidentiality, integrity, availability of the information based on the unique threats and exposures that face your application.
3. Implement error-handling in a manner that denies processing on any failure or exception.
4. All input fields must be validated before accepting. Input should be checked to prevent the program from executing malicious code. Input length must be validated to determine if it is within the predetermined minimum and maximum ranges. Input values should be screened for valid data types (e.g., number or character only, no special characters).
5. Output fields must be sanitized to ensure the output does not reveal too much information that could be used by malicious intent (e.g., default system-generated messages should be translated by the application). If invalid user input is encountered, the error message should not reveal the specific component which caused the error. Messages should be general in nature, and not reveal anything more than what is necessary.

6. The identity of the user must be authenticated if the application has access to non-public information. All user credentials and passwords must meet the security policy requirements for strength, change, and history. User access and capability must be limited to the functions required for the authorized access level only.
7. The requesting and granting of user accounts must include an approval process that validates the user and the minimum necessary access levels.
8. Establish security settings commensurate with the type of access.
9. All external systems (including web services), which require access to the application, must be authenticated and permissions checked before the external system becomes trusted.
10. All password entry fields should not "echo" the password in readable text when it is entered. Auto-complete of password fields should be disabled.
11. All sessions should be terminated when the user logs out of the system.
12. If a web application needs to store temporary or session-related information that is CONFIDENTIAL or RESTRICTED outside of the secured agency internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by Office of the CIO.
13. All web applications are required to have a security scan and test of the application on a recurring basis as determined by the state information security officer. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the state information security officer, agency information security officer, and IT management. Some packaged web applications where the package's architecture inherently protects the application from security risks, may have reduced testing requirements versus other web applications.
14. The anonymous public facing environment shall contain publicly approved content only. All non-public data and applications shall be segregated by additional firewalls and network monitoring.

Other application security recommendations and development guides can be reviewed at the OWASP or SANS websites:

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

http://www.sans.org/top25-software-errors/

8-606. Staff Use of Cloud Storage Websites

Accessing online cloud storage websites such as Dropbox, Google Drive, etc., is a security risk that will be restricted based on an employee's job functions. Use of these systems for any state purposes is prohibited unless approved by the employee's supervisor or manager. Even if approved, it is prohibited to process or store any CONFIDENTIAL or RESTRICTED information with these services, unless the storage is encrypted with approved technology, and has been approved in advance by the state information security officer.

8-607. Cloud Computing Standard

1. DEFINITIONS

1.1 NIST Definition of Cloud Computing

This standard incorporates the following definition from the National Institute of Standards and Technology (*The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, September 2011 [footnotes omitted]):

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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

***On-demand self-service*.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

***Broad network access*.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

***Resource pooling*.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

***Rapid elasticity*.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

***Measured service*.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

***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 either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. 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.

***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, libraries, services, 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 configuration settings for the application-hosting environment.

***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, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

***Private cloud*.** The cloud infrastructure is provisioned for exclusive use by a single organization comprised of 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.

***Community cloud*.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, 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).

1.2 Other Deployment Models

Government community cloud. A community cloud infrastructure provisioned solely for use by federal, state, and/or local government.

State cloud. The private cloud infrastructure provided by the Office of the CIO.

2. STANDARD

The following table contains the acceptable uses of cloud computing by state agencies. The classification of the data to be processed or stored using cloud computing determines the acceptable options. If there is a mix of data classifications, the most restrictive data classification must be used.

Data Classification	Cloud Deployment Models					
	State Cloud	Private Cloud	Government Community Cloud	Community Cloud	Public Cloud	Hybrid Cloud
RESTRICTED	✓	△	△	△	⊘	△
CONFIDENTIAL	✓	△	✓	△	⊘	△
MANAGED ACCESS PUBLIC	✓	✓	✓	✓	✓	✓
PUBLIC	✓	✓	✓	✓	✓	✓

(✓) means an approved deployment model for cloud computing;
(⊘) means an unapproved deployment model for cloud computing; and
(△) means prior approval by the Office of the CIO is required.

2.1 **Prior Approval Process**

An agency requesting prior approval of a cloud computing service must submit a service request to the Office of the CIO Service Desk. The request should provide detailed information about the cloud deployment model and data to be processed or stored using cloud computing. The Office of the CIO will respond to the request within four business days. The Office of the CIO may approve the request, approve the request with conditions, deny the request, or request additional information.

3. EXEMPTION FOR EXISTING SERVICES

Cloud computing services in use on December 31, 2017, are exempt from the requirements of this standard. The exemption for an existing service ends when either: (1) the current term of the agreement for such service expires; or (2) there are significant changes to the service.

4. FedRAMP COMPLIANCE

If the cloud service provider (CSP) does not have an official FedRAMP certification by an accredited third-party assessor organization (3PAO) and the CSP may store or process any CONFIDENTIAL or RESTRICTED data, the following conditions must be met or addressed in an agreement with the CSP:

1. The cloud service provider or third-party host (CSP/3PH) must provide evidence of secure storage of access credentials that are at least equal to that of state's internal systems.
2. Access to the cloud service must require multi-factor authentication based on data classification levels.
3. De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials.

4. Information must be encrypted using IT approved technology for information in transit as well as information stored or at rest.
5. Encryption key management will be controlled and managed by the state unless explicit approval for key management is provided to CSP/3PH by the agency.
6. All equipment removed from service, information storage areas, or electronic media that contained state information must have the information purged using appropriate means. Data destruction must be verified by the state before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse. A certificate of destruction must be provided for equipment that has been destroyed.
7. CSP/3PH must provide vulnerability scanning and testing on a schedule approved by the state information security officer. Results will be provided to agency.
8. Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at state.
9. CSP/3PH must meet all state requirements for chain of custody and information breach notification. CSP/3PH will maintain an incident management program that notifies the state within one (1) hour of a breach.
10. CSP/3PH will provide evidence of audit and assessment of the security of the service environment, and will agree to reasonable inspection of such security by gency-authorized parties.
11. CSP/3PH is required to advise the state on all geographic locations of stored state information. CSP/3PH will not allow state information to be stored or accessed outside the United States. This includes both primary and alternate sites.
12. Privileged access roles at the CSP/3PH are required to meet the same vetting standards of privileged access personnel at the state, such as background checks, etc.
13. CSP/3PH's must have SLAs in place that clearly define security and performance standards.
14. CSP/3PH will provide adequate security and privacy training to its associates, and provide the state information security officer with evidence of this training.
15. CSP/3PH will provide the state with the functionality to conduct a search of the data to meet public records requests.
16. Before contracting with a CSP/3PH, the state shall have proactive records planning in place to ensure the ability to have timely and actual destruction of records in accordance with Department record retention policies.

ARTICLE 7

AUDITING AND COMPLIANCE

8-701. Auditing and Compliance Security Standard

It is the responsibility of the state information security officer to ensure an appropriate level of security oversight is occurring at all potential exposure points of state and agency systems and operations so that the state has reasonable assurance that the overall security posture continuously remains intact. The state information security officer and agency information security officer have the responsibility to ensure the overall security program meets state and federal legal requirements.

The state information security officer will establish and manage an entity-wide oversight and compliance function. This will include, at a minimum, appropriate information security oversight at key points within the technology acquisition process, hardware and software change management process, and the contract management process when changes involve access to or potential exposure of CONFIDENTIAL or RESTRICTED information.

Compliance with this policy is mandatory. Any compromise or suspected compromise of this policy must be reported as soon as reasonably possible to appropriate agency management and the state information security officer.

An agency review to ensure compliance with this policy and applicable NIST 800-53 security guidelines must be conducted at least annually.

The state information security officer may periodically review agency compliance with this policy and the related NIST control framework. Such reviews may include:

- Reviews of the technical and business analyses required to be developed pursuant to this policy.
- Project documentation, technologies or systems which are the subject of the published policy or standard.

These additional reviews may occur due to significant changes in technical infrastructure, or to validate corrective actions after a security incident. All identified gaps or deficiencies must be documented in an agency security corrective action plan that shall be made available to the state information security officer as necessary. This plan is classified as a RESTRICTED information document, and should contain detailed descriptions of the security deficiencies, recommended remediation or mitigation activity, key milestones and target dates, and responsible parties. This plan should be a regular item for review by senior agency and Office of the CIO management to ensure acceptable progress is being made on mitigating or remediating security gaps.

8-702. Awareness and Training

The state provides information technology resources to authorized users to facilitate the efficient and effective performance of their duties. The use of such resources imposes certain

responsibilities and obligations subject to state government policies and applicable state and federal laws. It is the responsibility of all staff to protect information resources and ensure that such resources are not misused.

An information security awareness program must be developed, implemented, documented, and maintained that addresses the security education needs of the state. To ensure staff is knowledgeable of security procedures, their role and responsibilities regarding the protection of agency information and the proper use of information processing to minimize security risks, all staff with access to agency information must receive security awareness training, which must be reinforced at least annually. Technical staff must be trained to a level of competence in information security that matches their duties and responsibilities.

New Hire and Refresher Training

All new hires must complete security training, including information about this policy, as part of their orientation. On an annual basis, all staff must complete a security and privacy training session. The state will maintain records of all attendance for new hire and refresher training.

Periodic Briefings

Management should periodically incorporate information security topics into their meetings with staff. Additionally, the state information security officer may require periodic security briefings to selected audiences when circumstances require, such as responding to a gap in security policy or addressing recurrence of security incidents.

8-703. Security Reviews and Risk Management

This policy is based on the NIST 800-53 Security Controls framework. Pursuant to that framework, the state must conduct an annual review of the information technology environment to ensure compliance with these standards. The security controls that are to be inspected are organized into control families within three classes (management, operational, and technical).

The state information security officer will facilitate and oversee an annual security control assessment. This assessment will cover at least 1/3 of the control areas defined in the NIST 800-53 Security Controls, such that over a three-year timeframe all control areas will have been assessed.

This review must be conducted for each major system used within the state, and must include all infrastructure and peripheral processes that are used to support state business processes.

Unscheduled Risk Assessments

Unscheduled risk assessments may be performed at the discretion of the state information security officer or agency information security officer, typically when circumstances require additional oversight, such as after a security incident, increased security threat, or significant changes to the IT infrastructure. These assessments are flexible in nature, and are intended to review specific elements that have been identified as exception-based or high priority. These reviews can also be performed to validate the appropriate remediation or mitigation of a previous finding.

The security officer shall document the business area, reason for the review, scope of inspection, and dates of the review in the corrective action planning documentation. All findings and results will also be documented in the security corrective action plan.

8-704. Logging and Review of Auditable Events

All systems that handle CONFIDENTIAL or RESTRICTED information, allow interconnectivity with other systems, or make access control (authentication and authorization) decisions, must record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including on what system the activity was performed?
- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

Log Format, *S*torage, and Retention

The state is required to ensure the availability of audit log information that is subject to federal audit by allocating sufficient audit record storage capacity to meet policy requirements. Office of the CIO and the agency IT teams shall perform annual capacity planning and trend analysis to reduce the likelihood of such capacity being exceeded. The capacity and utilization of log files must be regularly monitored and reported, and action will be taken to keep an approved level of free space available for use. Automated notification of agency or Office of the CIO personnel must occur if the capacity of log files reaches defined threshold levels, or the audit logging system fails for any reason.

The audit logging process is required to provide system alerts to appropriate agency or Office of the CIO personnel in the event of an audit processing failure (e.g., shut down information system, unintended overwriting of the oldest audit records, stop generating audit records). All system logs must be sent to a central log review system that is protected from unauthorized access and is backed up for availability and integrity purposes. All log files subject to federal audit requirements must be retained for seven years.

Auditable Events

Security safeguard regulations require logging and reviewing events that are determined to have a moderate or above level of risk. Auditable events may be incorporated into system auto logs and change management documents. The following events should be logged and reviewed on a weekly basis:

- Log on and off the system;
- Change of password;
- All system administrator commands, while logged on as system administrator;
- Switching accounts or running privileged actions from another account (e.g., Linux/Unix SU or Windows RUNAS);

- Creation or modification of super-user groups;
- Subset of security administrator commands, while logged on in the security administrator role;
- Subset of system administrator commands, while logged on in the user role;
- Clearing of the audit log file;
- Startup and shutdown of audit functions;
- Use of identification and authentication mechanisms (e.g., user ID and password);
- Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
- Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;
- Changes made to an application or database by a batch file;
- Application-critical record changes;
- Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
- All system and data interactions concerning FTI;
- Additional platform-specific events, as defined by agency needs or requirements;
- Detection of suspicious or malicious activity such as from an intrusion detection or prevention system (IDS/IPS), anti-virus system, or anti-spyware system; and
- Physical entrance or access to secured and restricted areas or facilities where system and network infrastructure reside.

Audit Log Contents

Audit logs must contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The logs must identify or contain at least the following elements, or enough information in which to infer the following elements with reasonable assurance:

- Type of action (e.g., authorize, create, read, update, delete, and accept network connection);
- Subsystem performing the action (e.g., process or transaction name, process or transaction identifier);
- Identifiers (as many as available) for the subject requesting the action (e.g., user name, computer name, IP address, and MAC address). Note that such identifiers should be standardized to facilitate log correlation;
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time;
- Whether the action was allowed or denied by access-control mechanisms;

- Description or reason-codes of why the action was denied by the access-control mechanism, if applicable; and
- Depending on the nature of the event that is logged, there may be other information necessary to collect.

Audit Review, Monitoring, Findings and Remediation

Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. Additionally, these logs must be reviewed by authorized personnel to facilitate investigations of suspicious activity or suspected violations. All reports of findings must be reported to appropriate officials who will prescribe the appropriate and necessary actions.

- Logs of suspicious activity must be reviewed as soon as possible.
- Logs of system capacity and log integrity must be reviewed on a weekly basis.
- Logs of privilege access account creation or modification must be reviewed on a weekly basis.
- All other logs must be reviewed at least monthly.

When possible, the agency or Office of the CIO will employ automated mechanisms to alert the Office of the CIO, state information security officer, or agency information security officer when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis must not change the underlying log structure. It is acceptable for log analysis tools to extract data for analytical review, if the original audit logs remain unchanged and secured.

All relevant findings discovered because of an audit log review must be listed in the appropriate problem tracking system or the corrective action planning process to ensure prompt resolution or appropriate mitigating controls. All results and findings generated by the audit or review process must be provided to appropriate agency management within one week of completion. This report should be considered CONFIDENTIAL information.

Application Logging Review and Monitoring

All state applications must provide logging for security events. Application logs are invaluable data for identifying security incidents, monitoring policy violations, establishing baselines, providing information about problems and unusual conditions, contributing additional application-specific data for incident investigation which is lacking in other log sources, and helping defend against vulnerability identification and exploitation through attack detection.

Application logging content must be part of the overall system analysis and design activity, and should consider:

1. Application process startup, shutdown, or restart;
2. Application process abort, failure, or abnormal end;
3. Significant input and output validation failures;

4. Business process monitoring (e.g., activity abandonment, transactions, connections, information requests);
5. Audit trails (e.g., data addition, modification and deletion, data exports);
6. Performance monitoring (e.g., data load time, page timeouts);
7. Compliance monitoring and regulatory, legal, or court ordered actions;
8. Authentication and authorization successes and failures;
9. Session management failures;
10. Use of higher-risk functionality (e.g., addition or deletion of application credentials, changes to privileges, assigning users to tokens, adding or deleting tokens, submission of user-generated content - especially file uploads); and
11. Suspicious, unacceptable or unexpected behavior.

Application logs must be reviewed at least monthly. Corrective actions to address application deficiencies must be managed through the application development process or the applicable corrective action planning process.

8-705. Security Requirements for External Service Providers

All external service providers with access to CONFIDENTIAL or RESTRICTED information must have a written agreement that includes the minimum security requirements necessary for the protection of this information.

The state information security officer may inspect these external service provider arrangements to ensure compliance with state policies and requirements.

ARTICLE 8

VULNERABILITY AND INCIDENT MANAGEMENT

8-801. Incident Response

Computer systems are subject to a wide range of mishaps; from corrupted data files, to viruses, to natural disasters. These incidents can occur at any time of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other ways (e.g., disaster recovery plans). Responses to an incident can range from recovering compromised systems to the collection of evidence for a variety of forensic requirements. Preparation and planning for incidents, and ensuring the right resources are available, are critical to the state's ability to adequately detect, respond and recover from security incidents.

All agencies that process, store, or access CONFIDENTIAL or RESTRICTED information are required to maintain an incident response plan. This plan must include operational and technical components, which provide the necessary functions to support all the fundamental steps within the incident management life cycle, including the following:

1. Preparation;
2. Incident Triage and Identification;
3. Containment;
4. Incident Communication;
5. Preservation of Evidence;
6. Root Cause Analysis; and
7. Recovery and Permanent Remediation.

The security policy requires the establishment and maintenance of a computer security incident response capability that is in effect 24x7. This document identifies key steps for reporting security incidents and establishes formal reporting requirements for all such instances to the state's senior management and agency officials responsible for reporting to federal offices.

These procedures also describe the way Office of the CIO or agency technical staff will aid the in the eradication, recovery, and permanent remediation of the root cause of the incident. This is important to preserve as much evidence as practical while keeping in mind that prevention of damage is of the highest priority.

A. <u>Preparation - Scope and Responsibilities</u>

A security incident is any adverse event whereby some aspect of the state infrastructure is threatened (e.g., personal violation, loss of data confidentiality, disruption of data integrity, denial of service, security breach). It is important to note that even if there is no evidence of information being accessed by unauthorized personnel, exposing sensitive information in an unsecure manner is considered a security incident. For example, any unencrypted e-mail containing CONFIDENTIAL or RESTRICTED information (e.g. Federal Tax Information, Personally Identifiable Information) sent outside the secured state network is a security incident and should be reported as such.

All security incidents must be reported to the state information security officer, agency management, and the Office of the CIO Service Desk immediately. Security incidents will be tracked by the state information security officer. Any state staff who observe, experience, or are notified of a security incident, should immediately report the situation to the agency information security officer, state information security officer or the Office of the CIO Service Desk, but at the very least to their supervisor. All state management are responsible to ensure that their staff understand that awareness of the incident are to be reported immediately.

State Information Security Officer and Agency Information Security Officer

The security officers are responsible for assembling, engaging, and overseeing the incident response team. They will coordinate the management of security incidents and any identified follow-up activity, remediation, or countermeasures. They are also responsible for taking lead with information technology personnel to perform analysis and triage of incident impact and reportable conditions.

The security officers will finalize and sign off on any security incident reports, and determine follow-up activity, root cause analysis, long term mitigation, and updates to the security awareness training.

Agency information security officers are also responsible for ensuring that all technical areas within the agency have an understanding and ability to meet this standard. They are required to perform education and training of this standard to all applicable agency personnel, and then test the incident response process annually.

Incident Response Team

The state information security officer will identify key personnel who will serve as members of the state incident response team. This team will be made up of knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to state information systems, networks and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. This team may change from time to time, depending on the nature of the incident and the skills necessary to recover from it. Agencies may also identify additional incident response teams for their specific environment. The state information security officer or agency information security officer will maintain a contact list which includes the names, telephone numbers, pager numbers, mobile telephone numbers, email addresses, organization names, titles, and roles and responsibilities for all potential key incident response resources. Key responsibilities for the incident response team include:

- The state's priority is "Prevention over Forensics". In other words, do not allow a damaging incident to continue so that additional evidence may be collected.
- Conduct the initial triage. Perform a damage and impact assessment and document the findings.
- Report to state of agency management on a regular schedule with status and action plans.
- Maintain confidentiality of the circumstances around the incident.

- Follow procedures to maintain a chain of trust and to preserve evidence.
- Initiate the root cause analysis; bring in other resources as necessary.
- Initiate return to normal operations; bring in other resources as necessary.

B. Incident Management Procedures

Incident management procedures require, first and foremost, prevention of damage from the incident over forensics. This means that the priority is to shut off or terminate any potential damaging threat. It is strongly desired to perform this action in a manner that allows for detailed forensics or preservation of evidence, but if there is ANY doubt, all state personnel, whether employees or contractors, are required to disable the threat immediately. Following the assessment and termination of the threat, the next priority is containment, followed by recovery actions, damage determination, report documentation, lessons learned, and implementation of corrective actions.

All communication related to the incident should be carefully managed and controlled by the Office of the CIO and agency senior management. All personnel involved any incident management support activity will communicate only with the parties necessary for incident analysis or recovery activity, and to the state information security officer, Office of the CIO, or the agency information technology team. No other communication, unless explicitly authorized, is allowed.

A security incident report is classified as RESTRICTED information.

C. Incident Management Training and Testing

Annually, the state information security officer and agency information security officers shall provide training for appropriate identification, management, and remediation of an incident and shall facilitate a simulated incident response and recovery test for the state or agency security incident response team. This test will simulate a variety of security related incidents.

D. Incident Triage and Identification

As soon as an incident is suspected, personnel qualified and designated to respond shall be notified to take immediate action, determine incident impact, file a ticket, or prepare a report.

Initial triage will be conducted by the state information security officer/agency information security officer, Office of the CIO Service Desk, or the information technology team to understand the scope and impact of the incident and initiate appropriate action. Once an incident has been identified and reported, the state information security officer/agency information security officer will assume oversight of the incident response and will continually assess the incident conditions and determine if escalation of response actions is appropriate. Prevention of damage is given priority over forensics of incident source. Therefore, the state information security officer/agency information security officer and IT management may quarantine any potentially threatening system and terminate any threatening activity. The state information security officer will ensure that a security incident report is completed for all incidents.

For more complicated incidents that may require further analysis, the incident response team will be assembled via direction from the state information security officer, Office of the CIO, agency information security officer, or agency IT management. This team will take over the triage and impact assessment process.

A damage analysis of security incidents is to be initiated immediately after assessment by the state information security officer or the incident response team. They will determine if the incident impacts organizations outside of the agency's internal network. They will also determine if any reportable conditions, such as unauthorized disclosure of CONFIDENTIAL or RESTRICTED information exists. If the incident appears to have any citizen information compromised, immediate notification to the agency management, state information security officer, and agency information security officer is required. Agency management will oversee and coordinate all communication actions.

All forms of unauthorized disclosure of CONFIDENTIAL or RESTRICTED information, including the potential for unauthorized disclosure (such as information spillage), will be considered incidents. Information spillage refers to instances where either CONFIDENTIAL or RESTRICTED information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, an incident has occurred and corrective action is required.

E. Incident Containment

Any IT resources that are engaged in active attacks against other IT resources must be isolated and taken off the state network immediately. Incidents involving the exposure, or potential exposure, of CONFIDENTIAL or RESTRICTED information to unauthorized parties must also be contained immediately. Other compromises must be contained as soon as practical, considering impacts of service interruptions, recovery of equipment, and potential impacts of the incident itself.

Containment can be achieved by immediately disconnecting the resource from the network, revoking user access, or other means as appropriate. The state information security officer has the authority to coordinate with the Office of the CIO to block compromised services and hosts that present a threat to the rest of the state network. Notifications of outages or service interruptions will follow normal Office of the CIO or agency procedures if possible, but will not delay the outage or interruption if an attack or breach is underway or if the threat of an attack or breach is imminent.

F. Incident Communication

Reportable conditions, such as the breach of PHI, PII or FTI, require notification within specific timeframes as defined in state and federal law. It is the responsibility of the state information security officer and agency information security officers to understand these requirements and ensure the state and agency remain compliant in the event of a reportable incident.

Additionally, communication during a security incident must be carefully controlled to ensure that information that is disclosed is accurate, timely, and provided only to appropriate audiences.

It is the responsibility of the state information security officer, agency information security officer, Office of the CIO, and agency management to ensure that all communication regarding any security incident is managed and controlled.

G. Preservation of Evidence

In the event of a discovery of a breach of system security protections, an internal security investigation must be properly performed to preserve evidence. If the incident involves any type

of law enforcement, the incident response team will work with law enforcement to secure the potential evidence without reviewing additional content. Network hardware, software or data may be considered potential evidence.

The chain of custody steps that should be taken to preserve all potential evidence in the event of a security breach are as follows:

a. If possible, isolate the system from the network, either physically (unplug the network cable), or logically. Do NOT power the system off. Evidence in system memory may be lost.

b. If the system cannot be taken off the network, take pictures and screenshots.

c. Notify the agency information security officer immediately after initial steps, but no later than one hour after becoming aware of the possible incident.

d. Make a bit copy of the drive before investigating (e.g., opening files, deleting, rebooting).

e. Dump memory contents to a file.

f. Label all evidence.

g. Log all steps.

H. Incident Documentation and Root Cause Analysis

An incident report is required for all incidents except those classified as having a low impact to the state network. The incident report should include entry of the root cause, actions taken and any remediation or mitigation strategy to reduce the risk of recurrence. Depending on the nature of the security incident, a post-mortem meeting may be conducted.

Documentation of information is critical in situations that may eventually involve authorities as well as provides documentation of the actions taken to resolve the event. Incident reports are RESTRICTED information.

A formal root cause analysis must be performed within two weeks of the occurrence of the incident. This analysis should identify the core issues of the incident in the affected environment and actions that can be taken to address these issues. This can include physical, logical, or environmental changes, operational or administrative control changes, or enhanced training, education, or awareness programs.

I. Incident Recovery and Permanent Remediation

The incident response team, working with technology, application and data owners, shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems will be limited to authorized personnel until the security incident has been contained and root cause mitigated. Analysis and mitigation procedures must be completed as soon as possible, recognizing state systems are vulnerable to other occurrences of the same type.

The Office of the CIO, state information security officer, and agency information security officer shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations. Recovery procedures:

- Reinstalling compromised systems from trusted backup-ups, if required;

- Reinstalling system user files, startup routines, or settings from trusted versions or sources, if required;
- Validating restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons; and
- Increasing security monitoring and heighten awareness for a recurrence of the incident.

8-802. Penetration Testing

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to state penetration testing and intrusion testing. Penetration and intrusion testing will be conducted at the request of the agency or data owner(s) to determine if unauthorized access and or changes to an application can be made.

The results of the penetration and intrusion testing will be reviewed in a timely manner by the state information security officer. Any vulnerability detected will be evaluated for risk by the agency and a mitigation plan will be created and forwarded to the state information security officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for penetration and intrusion testing must be coordinated by both entities.

Any penetration or intrusion testing must be performed by individuals who are authorized by the state information security officer and who have requested and received written consent from the Office of the CIO at least 24 hours prior to any testing or scanning. Agencies authorized to perform penetration and intrusion testing or vulnerability scanning must have a process defined, tested and followed to minimize the possibility of disruption. Any other attempts to perform tests or scans will be deemed an unauthorized access attempt.

8-803. Vulnerability Scanning

Systems that provide information through a public network, either directly or through another service that provide information externally (such as the World Wide Web), will be subjected to vulnerability scanning.

All servers will be scanned for vulnerabilities and weaknesses by the Office of the CIO before being installed on the state network. For both internal and external systems, scans will be performed at least monthly or after any major software or configuration changes have been made, to ensure that no major vulnerabilities have been introduced. Priority setting of vulnerabilities will be based on impact to the state and as referenced in the National Vulnerability Database (HTTP://nvd.nist.gov).

All web-based applications will be scanned for vulnerabilities and weaknesses before being promoted to a production environment or after any major upgrades or changes have occurred. Results of the vulnerability scan will be reviewed in a timely manner by the state information security officer. Any vulnerability detected will be evaluated for risk by the Office of the CIO or agency and a mitigation plan will be created as required and forwarded to the state information security officer. The tools used to perform these tasks will be updated periodically to ensure that recently discovered vulnerabilities are included.

Where an agency has outsourced a server, application or network services to another entity, responsibility for vulnerability scanning must be coordinated by both entities.

8-804. Malicious Software Protection

Software and associated controls must be implemented across agency systems, and logs monitored, to detect and prevent the introduction of malicious code into the state environment. The introduction of malicious code such as a computer virus, worm or Trojan horse can cause serious damage to networks, workstations and state data. Users must be made aware of the dangers of malicious code. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk.

For workstations, virus signature files must be updated at least weekly. On host systems or servers, the signature files must be updated daily or when the virus software vendor's signature files are updated and published. Security patches for software will be applied as defined by the change management process, but all software must have security patches applied as soon as possible.

8-805. Security Deficiencies

All security deficiencies reported or identified in any security review, scan, assessment, or analysis must be documented in the state or agency Security POAM. These gaps must be managed to mitigation, remediation, or approved risk acceptance.

ARTICLE 9

DATA SECURITY

8-901. State Data

Data is a critical asset of the State of Nebraska. All staff have a responsibility to protect the confidentiality, integrity, availability of data generated, accessed, modified, transmitted, stored or used by the state, irrespective of the medium on which the data resides and regardless of format.

Agencies are responsible for establishing and implementing appropriate managerial, operational, physical, and technical controls for access to, use of, handling of, transmission of, and disposal of state data in compliance with this policy, federal requirements, and any applicable records retention schedule. The agency data owner should carefully evaluate and determine the appropriate data sensitivity or classification category for their information. Assigning classifications determines day-to-day practices with information: how it is handled, who handles it, how it is transported, how it is stored, and who has access.

8-902. Data Classification Categories

Data owned, used, created or maintained by the state is classified into the following four categories:

(1) **RESTRICTED.** This classification level is for sensitive information intended for use by a limited number of authorized staff with an explicit "need to know" and controlled by special rules to specific personnel. Examples of this privileged access information include: attorney-client privilege information, agency strategies or reports that have not been approved for release, audit records, network diagrams with IP addresses specified, and privileged administrator credentials. This level requires internal security protections and could have a high impact in the event of an unauthorized data disclosure.

(2) **CONFIDENTIAL.** This classification level is for sensitive information intended for use within an agency and controlled by special rules to specific personnel. Examples of this type of data include: federal tax information (FTI), protected health information (PHI) and other Patient Medical Records covered by Health Insurance Portability and Accountability Act (HIPAA), payment card industry (PCI) information, and personally identifiable information (PII).

(3) **MANAGED ACCESS PUBLIC**. This classification level is for information that is public in nature but may require authorization to receive it. This type of information requires a minimal level of security and would not have a significant impact in the event of data disclosure. This type of information does not include personal information but may carry special regulations related to its use or dissemination. This data may also be data that is sold.

(4) **PUBLIC**. This classification is for information that requires no security and can be handled in the public domain.

8-903. Data Inventory

Each agency shall identify and classify all information according to this policy. Each agency shall maintain an inventory of where CONFIDENTIAL and RESTRICTED information reside, so those environments can be assessed for security adequacy.

8-904. Data Security Control Assessment

Each agency shall perform a security control assessment that assesses the adequacy of security controls for compliance with this policy and any applicable security frameworks (e.g., NIST, PCI, CMS, and IRS). The assessment may be performed internally by the agency information security officer or with the assistance of the state information security officer. Each agency is required to have an assessment at least once every year, covering at least one-third of the applicable controls such that all control areas have been assessed over a three-year period. Agencies are also required to perform an assessment anytime significant changes to the technical environment occur.

8-905. Data Sharing

It is critical that agencies that share information and systems learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It also is critical that they establish formally documented agreements regarding the management, operation and use of interconnections, as required. The agreement should be reviewed and approved by appropriate senior staff from each organization.

All agencies that share connectivity and information between the agency and the Office of the CIO are required to have a security program that meets this policy. The agency information security officer shall develop a system security plan that must be approved by the state information security officer. All agencies shall perform a security control assessment that identifies the adequacy of security controls and precautions for protecting state information. If the agency performs this assessment independent of the state information security officer, an approved and signed interconnection system agreement that describes the security controls and plans will be in place to protect state information.

8-906. Data Destruction

Agency data must be disposed of in accordance with the Records Management Act and any related records retention schedule. Disclosure of sensitive information through careless disposal or re-use of equipment presents a risk to the state. Formal procedures must be established to minimize this risk. Storage devices such as hard disk drives, paper or other storage media (e.g., tape, diskette, CDs, DVDs, USB drives, cell phones, and memory sticks) regardless of physical form or format containing CONFIDENTIAL or RESTICTED information must be physically destroyed or securely overwritten when the data contained on the device is to be disposed. These events should include certificates of destruction. State and agency asset management records must be updated to reflect the current location and status of physical assets (e.g., in service, returned to inventory, removed from inventory, destroyed) when any significant change occurs.

Sec.2. In section 5-204(2.2.6), strike the sentence beginning with “Section”.

Sec.3. Strike section 5-204(4) in its entirety.

Sec.4. In Attachment A to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.5. In Attachment B to section 5-204, strike the sentence beginning with “See NITC 8-101”; strike the bulleted sentence beginning with “Approved remote access”; and strike the subsection titled: “Identified NITC policies that apply to use, access and protecting information:” in its entirety.

Sec.6. Staff shall reformat and re-enumerate the provisions of this proposal for consistency prior to final publication.

Sec.7. Original sections 5-204, 8-101, 8-102, 8-103, 8-201, 8-301, 8-302, 8-303, 8-304, and 8-401 are repealed. Resource documents 8-RD-01, 8-RD-02, 8-RD-03, 8-RD-04, 8-RD-05, and 8-RD-06 are repealed.

Sec.8. This proposal becomes operative on December 1, 2017.

Nebraska State Accountability (NeSA- Reading, Math, Science and Writing)

PROJECT DESCRIPTION

Legislative Bill 1157 passed by the 2008 Nebraska Legislature required a single statewide assessment of the Nebraska academic content standards for reading, mathematics, science, and writing in Nebraska's K-12 public schools. The new assessment system was named Nebraska State Accountability (NeSA), with NeSA-R for reading assessments, NeSA-M for mathematics, NeSA-S for science, and NeSA-W for writing. The assessments in reading and mathematics were administered in grades 3-8 and 11; science was administered in grades 5, 8, and 11; and writing was administered in grades 4, 8, and 11.

PROJECT DETAILS

Project Manager: John Moon

Start Date: 07/31/2016
Finish Date: 06/30/2017

Total Estimated Costs:	Actual Costs to Date:	Estimate to Complete:
$4,329,379.00	$2,335,875.50	$1,993,503.50
		54%

PROJECT STATUS - June 2017

Overall	Schedule	Scope	Budget

NESA testing was completed May 5, 2017. DRC will deliver the test results to NDE on June 12 for pre-score resolution to be completed by June 23. After districts receive preliminary results on July 17 and review any corrections, district submit requests to NDE for Final resolution during the month of July. NDE will upload final data files to DRC August 4. DRC will provide final data files and reports to districts in the fall of 2017.

KEY ACCOMPLISHMENTS (since last report)

--

UPCOMING ACTIVITIES (in next reporting period)

--

PROJECT STATUS - April 2017

Overall	Schedule	Scope	Budget

NITC and DRC complained of packet loss and slowness on NeSA testing. Both DRC and Network Nebraska (NN) investigated the issue. NN shared the following information during the NITC meeting on April 11, 2017.

1. Network Nebraska engineers were alerted and began a sequence of diagnostics, including a trace route that showed DRC egress through Windstream Communications and ingress via Cogent Communications.

a. Thurs 12:19pm NN, "Everyone, I have not found any issues within the Network Nebraska transport core. I am double checking our cross connects with our service providers to verify that there are no issues there. I did just get off the phone with DRC and they have a tac team looking into the slowness issues. The tech I spoke with is currently looking at their database logs. I'll keep you updated."

b. Thurs 2:30pm NN, "Traces have been provided to DRC."

c. Thurs 3:42pm NN, "FYI - We are seeing Internet response issues impacting Network Nebraska partners. Our investigation is showing the issue outside of our network, within Cogent and/or AT&T provider. We are currently shifting traffic away from Cogent to see if we can get short-term relief while we investigate deeper. Customers were alerted using the Network Nebraska notification system."

d. Thurs 5:12pm NN, "Short-term we have removed Cogent as one of our providers and that resolved the response issue. A ticket was opened with Cogent to investigate further. We are currently routing all traffic through our other paths; Windstream, TransitRail-Commercial Peering Service (TR-CPS), Omaha Exchange, Internet2 and WiscNet. All looks good and we're monitoring."

e. Fri 9:42am NN, "Just FYI that our efforts to get information from Cogent is not going very well. We will keep checking back (pestering) for updates. So far today the traffic is being transported without issues using our other paths."

continued on key accomplishments...

KEY ACCOMPLISHMENTS (since last report)

f. Fri 9:55am NN, “We do not have any confirmation mainly due to a lack of information from Cogent. Their website (http://status.cogentco.com/) did not show any issues yesterday. We do know that eliminating Cogent as a traffic peer immediately resolved the performance and packet-loss issues that were reported.”
g. Fri 11:27am OCIO demanded ticket escalation with Cogent.
a. Sun 1:59pm Cogent requests follow up information.
b. Mon 10:16am NN to Cogent, “I have provided multiple destination networks with graphing showing packet loss. Universally and immediately after we deactivated the peering to you, our customers reported everything was back to normal. I would suggest looking at your peer points between you and your upstream providers to those destinations.”

continued on upcoming activities...

UPCOMING ACTIVITIES (in next reporting period)

c. Mon 5:07pm Cogent unable to open all of the attachments. Cogent, “Please send in another format or provide your source and destinations as well as which circuit in Omaha this trouble pertains to.”
d. Tues 10:47am Cogent escalates new trouble ticket.
e. Tues 3:25pm NO new updates from Cogent—Cogent Internet traffic still diverted through other pathways.
2. Further explanation from Cogent still required.
3. NDE is waiting for additional information.

Nebraska Regional Interoperability Network (NRIN)

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.

PROJECT DETAILS

Project Manager: Sue Krogman

Start Date: 10/01/2010
Finish Date: 08/31/2018

Total Estimated Costs:	Actual Costs to Date:	Estimate to Complete:
$10,024,084.90	$8,745,330.26	$1,278,754.64
		87%

PROJECT STATUS - June 2017

Overall	Schedule	Scope	Budget

More completed work.

KEY ACCOMPLISHMENTS (since last report)

St. Paul Courthouse, Oconto to Sumner is fixed.
Geneva to Fairbury is installed.
Half of Cass County is installed and the rest will be done along with the Motorola 800 MHz system.
Structurals are being done on towers from Beatrice to Tecumseh.
Line of Sites and path calculations are being done from Fremont into the Orion system just outside of Blair.

UPCOMING ACTIVITIES (in next reporting period)

Work on the South Central Region installation
Begin optimization of South Central Region equipment and software.
South Central Region Network Sign-off

PROJECT STATUS - April 2017

Overall	Schedule	Scope	Budget

Negotiations are still in the process for the KUTT tower in the SE Region as well as the KUSO tower in the NE Region. Each of these towers is a vital link in this build-out. Work is being done in conjunction with Motorola in Cass County. Village Board visitations were done for all of Cass County and agreements are being processed. The investment justification meeting will determine how many Homeland Security dollars this project will be receiving.

KEY ACCOMPLISHMENTS (since last report)

--

UPCOMING ACTIVITIES (in next reporting period)

--

Medicaid Management Information System Replacement Project (MMIS)

PROJECT DESCRIPTION

Nebraska's current Medicaid Management Information System (MMIS) has supported DHHS Medicaid operations since 1977. Medicaid is an ever-changing environment where program updates occur quickly. The need for access to data is increasing and technological enhancements are necessary to keep pace with program changes. Recognizing the need to implement new technology, and with the support of the Legislature, DHHS embarked on the planning phase for replacement of MMIS functionality.

PROJECT DETAILS

Project Manager: Don Spaulding

Start Date: 07/01/2014
Finish Date: 06/30/2020

Total Estimated Costs:	Actual Costs to Date:	Estimate to Complete:
$113,600,000.00	$6,679,044.00	$106,920,956.00
		6%

PROJECT STATUS - June 2017

Overall	Schedule	Scope	Budget

DMA RFP posted an Intent to Award to Optum Government Solutions, Inc. on December 30, 2016. Due to an upheld protest, a revised intent to Award contract to Deloitte Consulting LLP was posted on February 1, 2017. All protests have been closed.

Numerous Public Record Requests have been fielded and estimated but are on hold awaiting execution orders.

The Project Coordination Committee (PCC) and the MLTC Integration Team meet regularly formally addressing system integration across all MMIS Replacement Projects and related systems such as Eligibility and Enrollment.

Independent Verification and Validation (IV&V) activities with First Data Government Solutions, LP has been engaged.

KEY ACCOMPLISHMENTS (since last report)

- Deloitte contract negotiations are ongoing with a June target completion.
- DMA Readiness activities completed include business subject matter expert engagement, work track refinement, resource allocation and project management planning.
- Finalized drafts of CMS required DMA documents including IS&T Security Plan, Project Management Plan and Concept of Operations.
- DMA Communications accomplishments include Share Point site creation and publication of a monthly newsletter.
- IV&V DMA Monthly CMS status reporting has commenced.

UPCOMING ACTIVITIES (in next reporting period)

- Contract with the awarded vendor.
- Support public records request processes as required.
- Document DMA Proof of Need and Resource Mitigation Plan.
- DMA CMS Certification Checklist inclusion/exclusion methodology and MECL roadmap.
- Submit IAPD Update to CMS including Concept of Operations, IS&T Security plan and Project Management plan.
- Continue DMA readiness planning and preparation activities.

PROJECT STATUS - April 2017

Overall	Schedule	Scope	Budget

DMA RFP posted an Intent to Award to Optum Government Solutions, Inc. on December 30, 2016. Due to an upheld protest, a revised intent to Award contract to Deloitte Consulting LLP was posted on February 1, 2017. This opened a new protest period which is still in process.

Numerous Public Record Requests have been fielded and estimated but are on hold awaiting execution orders.

The Executive Steering Committee has chartered the Project Coordination Committee (PCC) and an MLTC Integration Project formally addressing system integration across all MMIS Replacement Projects and related systems such as Eligibility and Enrollment.

Independent Verification and Validation (IV&V) activities with First Data Government Solutions, LP has commenced.

Medicaid Management Information System Replacement Project (MMIS)

KEY ACCOMPLISHMENTS (since last report)

- The revised DMA Intent to Award to Deloitte Consulting LLP was posted on February 1, 2017.
- Deloitte contract negotiations have begun along with Deloitte work deliverables delineation.
- DMA Readiness activities including current state discovery documentation, facilities preparation, communications, resource allocation and project management planning are underway.
- The IV&V project was formally kicked off on March 21, 2017 with multi-project strategic development in process.

UPCOMING ACTIVITIES (in next reporting period)

- Support the formal protest and public records request processes.
- Document DMA Proof of Need.
- Contract with the awarded vendor.
- Submit IAPD Update to CMS including Concept of Operations, IS&T Security plan and Project Management plan.
- Continue DMA readiness planning and preparation activities.
- The PCC will continue planning work efforts to address overall MMIS Replacement module interoperability, system integration and DMA project preparation activities.

Medicaid Eligibility & Enrollment System

NITC Nebraska Information Technology Commission

PROJECT DESCRIPTION

The Affordable Care Act (ACA) included numerous provisions with significant information systems impacts. One of the requirements was to change how Medicaid Eligibility was determined and implement the changes effective 10/1/2014. As a result of the lack of time available to implement a long-term solution, the Department of Health and Human Services implemented a short-term solution in the current environment to meet initial due dates and requirements. This solution did not meet all Federal technical requirements for enhanced Federal funding but was approved on the assumption that a long-term solution would be procured. An RFP was developed and procurement has been completed with Wipro selected as the Systems Integrator for the IBM/Curam software.

PROJECT DETAILS

Project Manager: Don Spaulding

Start Date: 10/28/2014
Finish Date: 12/31/2018

Total Estimated Costs:	Actual Costs to Date:	Estimate to Complete:
$57,741,564.00	$21,301,064.00	$36,440,500.00 37%

PROJECT STATUS - June 2017

Overall	Schedule	Scope	Budget

Many areas of the design phase are coming to an end. Document deliverables are being produced and will be sent to State teams for review and feedback. Key areas of the design that are still active have been prioritized and resourced. Efforts on remaining design activities include Non- MAGI rules, MMIS interface and Portal design.

Milestones and Progress:

- Design - New proposed date 8/25/17 - 91% completed
- Data Conversion - New proposed date 9/18/17 - 65% completed
- Development - New proposed date 12/29/17 - 10% completed
- Testing - New proposed date 9/18//18 - 8% completed

KEY ACCOMPLISHMENTS (since last report)

Sprint testing launched in March and continued through April and May. As of May 15, State testing was completed for Sprints 1-4, and Sprints 5-7 are in progress. Sprints 8 and 9 were demonstrated and released to the State testing team. Additionally, the scope for sprints 10 and 11, which includes Notices and MAGI Evidences, were approved for development activity

MCI functional and technical documents have been delivered to the state team for review and feedback. The development and unit testing environment for the MCI is complete. The state team is using the MCI services for development and testing with NFOCUS.

The ACCESSNebraska Portal and Curam Citizen Portal work stream received the vision and direction from project leadership. An integrated approach will be designed and developed. The user experience and consolidated views of benefit information are of high importance.

UPCOMING ACTIVITIES (in next reporting period)

The Change Impact Assessment workgroup continues the analysis of impacted changes between the new and existing eligibility systems. Following State review and approval of the change registers, the vendor will analyze the change impacts, and create high level and detailed action plans. The initial preview of the Change Impact Register is June 14, 2017.

The Training Plan, which finalizes user roles, training delivery, breakdown of training modules, and templates is due June 15, 20

Interface development - Federal Data Services Hub (FDSH)

MMIS interface work sessions to map NTRAC data to MMIS data requirements. Understand if MMIS data requirements need historical data from the NFOCUS system converted to NTRAC.

Design phase document deliverables for SI payment are being produced. State teams will be reviewing the documents and providing feedback. The formal process will be followed to ensure the deliverable criteria is met.

Medicaid Eligibility & Enrollment System

PROJECT STATUS - April 2017

Overall	Schedule	Scope	Budget

The EES/ NTRAC project has undergone an extensive effort to establish a complete integrated master schedule that carries across phases. The complete master schedule shows the current target dates are unobtainable without significant risk. Additionally, the March 9th, 2017 milestone to complete design was not met. Project leadership has been engaged to evaluate the project schedule impacts. The master schedule was presented to the project steering committee on 4/4/17 and more information was requested to help determine next steps.

Design:

- Common Design (technical) - 89% completed
- Functional Delivery Unit Design (Curam) - 90% completed
- Data Conversion and Migration - 48% completed
- Business Rules Design - 95% completed

KEY ACCOMPLISHMENTS (since last report)

- Functional Delivery Unit (FDU) #5 is the last remaining Curam design work package remaining. The project team is packaging up the content for end to end design review work sessions.

- In March the first development sprint for Curam was demonstrated to the state team. State testing of sprint development releases for Curam has started.

- Abbreviated AR/PBR CMS review was conducted on February 17, 2017

- Mapping of 645 out of 854 data elements have been completed between MMIS, NFOCUS and NTRAC. The team is identifying data elements that NTRAC does not capture. A gap analysis will be performed to mitigate the data requirements.

- Integration test and system test environment and infrastructure documentation review by the state team. New environments are being configured.

UPCOMING ACTIVITIES (in next reporting period)

- Drafting the correspondence (notices and requests)

- IVR/ Cisco call tree design and data integration design work activities. Once the design document is complete a review session will be held and statement of work requested for development from Cisco.

- Business scenario / Use cases for design phase work will continue in the following work streams.
  - MCI - Master Client Index (data synchronization)
  - ACCESSNebraska & Curam Portal functional and technical integration
  - NTRAC and NFOCUS interface
  - IVR/ Cisco phone system integration
  - File Director integration

- Development for Curam sprints 4 - 8. Functional sprint demos and State testing of sprints will occur as they are released.

- Branding operating assumptions and design. Branding will include the citizen user experience coordination across NTRAC and associated solutions.

Enterprise Resource Management Consolidation

NITC | Nebraska Information Technology Commission

PROJECT DESCRIPTION

Migrate five current disparate IT systems individually supporting human resource and benefit management, employee recruiting and development, payroll and financial functions, and budget planning to a cloud-based single enterprise platform. The migration will include implementation of two new modules: E-Procurement and Budget Planning. The end state would be the realization of operational, process, and expense synergies by moving to a single enterprise platform at the end of this migration.

PROJECT DETAILS

Project Manager: Dovi Mueller

Start Date: 07/13/2017
Finish Date: 01/15/2020

Total Estimated Costs:	Actual Costs to Date:	Estimate to Complete:
$17,758,000.00		

PROJECT STATUS - June 2017

Overall	Schedule	Scope	Budget

Project has been approved by NITC, Governor, and has been briefed to the Appropriations Committee. Migration funding and appropriations were approved for the project with both funds being transferred and appropriations made available starting on July 1, 2017.

DAS has selected KPMG and Civic Initiatives as the migration contractors for this project. An initial kick off meeting was conducted on Tuesday, May 23, 2017 and a three-day project planning/campaign plan will be conducted on July 11-13, 2017. This meeting will formally establish the start date of this project and also establish the targeted implementation dates of the three phases over the next 2.5 years.

KEY ACCOMPLISHMENTS (since last report)

--

UPCOMING ACTIVITIES (in next reporting period)

--

PROJECT STATUS - April 2017

Overall	Schedule	Scope	Budget

Project has been approved by NITC, Governor, and has been briefed to the Appropriations Committee. Waiting on final budget determination if the full cloud migration will be approved or just the Oracle JDE 9.2 upgrade.

Once budget determination is made, then DAS will start engaging the vendors to start the migration planning.

KEY ACCOMPLISHMENTS (since last report)

--

UPCOMING ACTIVITIES (in next reporting period)

DAS Appropriations bill is voted in the legislature -- April 2017

Attachment 4-f

NITC Strategic Initiatives Status Report			
Strategic Initiative, Action Item and Deliverable/Target			
State Government IT Strategy		**Status**	**Notes**
1	**Single Help Desk Solution - Incident Management Implementation**		
1.1	Implement solution and migrate initial group of agencies.	Completed	
1.2	Migrate remaining agencies in phases.	In progress	Scheduled for completion by December 2017.
2	**Service Catalog Implementation**		
2.1	Create service catalog for OCIO.	Completed	
3	**Change Management Solution Implementation**		
3.1	Implement new change management process for OCIO.	Completed	Updated from “in progress” to “completed”
3.2	Add other cabinet agencies.	In progress	Updated from “not started” to “in progress”
4	**Enhance Information Security**		See IT Security Initiative.
5	**Enhanced Operations Center**		
5.1	Develop system performance reports and dashboards.	Completed	
5.2	Combine Operations and Help Desk.	Completed	
5.3	Implement fully functional 24/7 Operations Center.	Completed	
5.4	Migrate from Help Desk to Service Desk.	Completed	
5.5	Establish Problem Management process.	Completed	Updated from “in progress” to “completed”
5.6	Establish Service Manager Program.	Completed	
6	**IT Cost Efficiencies**		
6.1	Review process in support of the State’s IT spending.		See State IT Spending Analysis Initiative.
6.2	Assess environment, including existing infrastructure and applications, through Agency IT Plans.	Completed	
6.3	Enhance server virtualization and optimization.	In progress	
6.4	Implement a configuration management database (CMDB) and full asset management processes.	In progress	
6.5	Develop a Cloud Strategy		See Cloud Strategy Initiative.
6.6	Develop a Mobile Application Platform Strategy.	Completed	Updated from “in progress” to “completed”
7	**Operationalize IT and Project Governance**		

7.1	Enterprise Application governance (i.e., Service Desk tool)	Completed	
7.2	Enterprise Project Governance through the Project Management Office	Completed	
7.3	Enterprise Project Governance	Not started	
8	**Consolidate on STN Domain**		
8.1	Implement phased migration.	In progress	
9	**Data Center Consolidation - Agency Server Migration**		
9.1	Implement phased migration.	In progress	
10	**Initiate Active/Hot Standby Solution - Enterprise Apps**		
10.1	Install core network equipment at both locations.	Completed	
10.2	Implement phased migration.	In progress	
Cloud Strategy		**Status**	**Notes**
1	**Develop a strategy for the use of cloud-based services by Nebraska state government.**		
1.1	Cloud Strategy Document	In progress	Part of security policy scheduled for adoption at the July meeting.
State IT Spending Analysis		**Status**	**Notes**
1	**Create new accounting codes to better capture IT-related spending.**		
1.1	Develop new accounting codes and definitions.	Completed	
1.2	Pilot test new codes.	Completed	
1.3	Roll-out new codes to cabinet agencies.	Completed	
2	**Develop reporting tools using the new accounting codes.**		
2.1	Design reports to be generated by the accounting system using the new codes.	In progress	
3	**Prepare an analysis of information technology spending by Nebraska state government.**		
3.1	IT Spending Analysis Document	Not started	
IT Security		**Status**	**Notes**
1	**Complete Mobile Device Management solution implementation (MaaS360 from Fiberlink / IBM).**		

1.1	MaaS360 will be installed on all mobile devices authenticating to the State of Nebraska network.	In progress	An alternative solution has been selected.
2	**Complete transition to Security Mentor Security Awareness videos for all State employees.**		
2.1	Security Awareness videos will be delivered to all State employees through the Learning Management System on a semi-monthly basis.	Completed	
2.2	Emails that re-inforce the video will be sent to all State employees on the off months.	Completed	
3	**Perform a complete IT hardware inventory of all State agencies.**		
3.1	Itemized list of IT-related hardware used within the State of Nebraska network	In progress	
4	**Perform a complete IT application inventory of all State agencies.**		
4.1	Itemized list of applications used within the State of Nebraska network	In progress	
5	**Complete Nebraska Security Operation Center.**		
5.1	Enterprise Security Information and Event Management (SIEM) system	In progress	
5.2	Enterprise Security Operations Centers in multiple locations 24 x 7 for redundancy	Not started	
5.3	Service Level Agreements with all participants	Not started	
5.4	Written Charter	Not started	
6	**Complete update of NITC standards and guidelines according to gap analysis**		
6.1	Updated NITC 8-101 Information Security Policy	In progress	New security policy scheduled for adoption at the July meeting.
6.2	Updated NITC 8-102 Data Security Standard	In progress	
6.3	Updated NITC 8-103 Minimum Server Configuration Standard	In progress	
6.4	Updated NITC 8-201 Information Technology Disaster Recovery Plan	In progress	
6.5	Updated NITC 8-301 Password Standard	In progress	
6.6	Updated NITC 8-303 Remote Access Standard	In progress	
6.7	Updated 8-304 Remote Administration of Internal Devices Standard	In progress	

Strategic Initiatives

In order to advance its vision and goals, the NITC, with input from its advisory groups and other stakeholders, has identified nine key initiatives which promote the effective use of technology within the State of Nebraska, as well as education, economic development, local government, and health care. By emphasizing selected strategic initiatives, the NITC hopes to encourage funding of these initiatives and to encourage state agencies to work together to advance these initiatives.

The first four strategic initiatives—State Government IT Strategy, Cloud Strategy, IT Security, and Nebraska Spatial Data Infrastructure (NESDI)—further the development of an enterprise approach to IT in order to achieve the State's IT priorities of security, availability, and consolidation. The fifth initiative, State IT Spending Analysis, establishes a process for better tracking State IT expenditures. This initiative will enable better decision-making regarding IT investments.

Four strategic initiatives—Network Nebraska, Digital Education, Community IT Development, and eHealth—promote the effective use of technology in these sectors. The initiatives also highlight the need to address the divide between those with access to technology and the skills to effectively use it and those without.

A brief description of each strategic initiative follows:

State Government IT Strategy. The objective of this initiative is to develop and implement a comprehensive strategy for the use of information technology by Nebraska state government. The strategy will utilize a hybrid centralization model combining elements of both the centralized and decentralized IT management models. Enterprise technologies will be centralized with agency-specific activities remaining with the agencies.

Cloud Strategy. This initiative will develop a comprehensive strategy for the use of cloud-based services by Nebraska state government. Research shows that organizations with an enterprise-wide cloud strategy are far more successful at using the cloud to reduce costs, improve efficiency, and increase business agility.

State IT Spending Analysis. The objective of this initiative is to gain a better understanding of information technology spending by Nebraska state government. Action items include creating new accounting codes to better capture IT-related spending, developing reporting tools using the new accounting codes, and preparing an analysis of IT spending by Nebraska state government.

IT Security. This initiative will define and clarify policies, standards and guidelines, and responsibilities related to the security of the State's information technology resources.

Nebraska Spatial Data Infrastructure (NESDI). The objective of this initiative is to develop and foster an environment and infrastructure that optimizes the efficient use of geospatial technology, data, and services to address a wide variety of business and governmental challenges within the state. Geospatial technologies and data will be delivered in a way that supports policy and decision making at all levels of government to enhance the economy, safety, environment and quality of life for Nebraskans.

Network Nebraska. In order to develop a broadband, scalable telecommunications infrastructure that optimizes the quality of service to every public entity in the state of Nebraska, the Office of the CIO and the University of Nebraska engaged in a collaborative partnership that used existing and new resources to aggregate disparate networks into a multipurpose core backbone extending from Omaha, Lincoln, Grand Island to Scottsbluff.

In order to advance its vision and goals, the NITC, with input from its advisory groups and other stakeholders, has identified nine key initiatives which promote the effective use of technology within the State of Nebraska, as well as education, economic development, local government, and health care.

Strategic Initiatives

Benefits of Network Nebraska include lower network costs, greater efficiency, interoperability of systems providing video courses and conferencing, increased collaboration among educational entities, new educational opportunities, more affordable Internet access, and better use of public investments. Nearly all (99.6%) Nebraska public school districts and all public higher education entities participate in Network Nebraska, benefitting from one of the lowest commodity Internet rates in the entire country. Network Nebraska's low commodity Internet rates are made possible through aggregation of demand and statewide bidding. Network Nebraska's new action item focus will be on better performance metrics and more effective communication to participants and stakeholders.

Digital Education. The primary objective of the Digital Education Initiative is to promote the effective and efficient integration of technology into the instructional, learning, and administrative processes and to utilize technology to deliver enhanced digital educational opportunities to students at all levels throughout Nebraska on an equitable and affordable basis. This initiative will involve the coordination and promotion of several major systems and applications that have either been developed mostly at the local level or have not been replicated statewide. Action items will focus on creating professional development opportunities for Nebraska educators to maximize student success through the innovative uses of technology in teaching, addressing technical challenges for students in the transition from secondary to post-secondary education, and addressing the need for equitable broadband access for students and their families to access digital education resources.

Community IT Planning and Development. In order to support community-based efforts to address broadband availability, broadband adoption, and the development of a skilled IT workforce, the NITC Community Council has built partnerships with other organizations to develop and deliver outreach programs. Action items include supporting the efforts of communities to address broadband-related development by recognizing outstanding programs and developing a series of best practices and case studies. The Community Council will also partner with the Education Council to expand awareness and address equitable access to broadband for students and their families.

eHealth. The Nebraska Information Technology Commission formed the eHealth Council in 2007 to make recommendations on how the State of Nebraska can effectively and efficiently promote the adoption of interoperable health technologies. On July 27, 2015, the Nebraska Information Technology Commission received $2.7 million in funding from the Office of the National Coordinator for Health Information Technology to advance health information exchange in the state through NeHII (Nebraska Health Information Initiative). The implementation of the two-year grant will be the focus of this initiative.