North Dakota Board of Higher Education
Meeting Notice and Agenda
January 29, 2015

The State Board of Higher Education will meet on Thursday, January 29, 2014, 11:00 a.m. CT, Bismarck State College, NECE building, EGC 335, 1200 Schafer Street, Bismarck, ND 58506. The live video stream can be viewed at: http://www.ndus.edu/board/live-stream/.

Call to Order

1. Approval of Agenda
2. Approval of Meeting Minutes
   • November 20, 2014
   • December 9, 2014

Reports and Public Comment
3. NDUS Information Technology Security Audit and Vulnerability Assessment – State Auditor Office
4. Board Chair’s Report – Temporary Board Chair – Hjelmstad
   • Appointment of Committee Members
   • Update on Challenge Fund Grant Program – Kathleen Neset
5. Interim Chancellor’s Report – Interim Chancellor Skogen
6. Institutional Reports
7. North Dakota Student Association Report – Zachary Niebuhr
9. Staff Senate Report – Emma Tufte
10. Public Comment

Board Business
11. Elect Board Chair
12. Approve Roles and Responsibilities Report – Interim Chancellor Skogen
13. Legislative Update and SBHE Action on Select Bills – Murray Sagsveen and Laura Glatt
14. Approval of Proposed Changes to Tuition Model Plan – Laura Glatt
15. LRSC Request to Name the Newly Constructed Technical Education Center – President Darling
16. Approve UND Agreement for Joint Exercise of Peace Officer Duties – Murray Sagsveen
17. Authorize SBHE Audit Committee as the Search Committee for New Chief Auditor Hire

SBHE Academic and Student Affairs Committee Recommendations – Chair Reichert
18. Committee Consent:
   I. Accept 2014 Accreditation Report
SBHE Budget and Finance Committee Recommendations – Chair Morton

19. Committee Consent:

I. Authorize WSC to seek 15-17 state general fund appropriation of $1,200,000; and, increase spending for the Workforce Training project from $8,238,267 to $9,438,267 funded from $1,700,000 general fund, $2,500,000 financed through the Bank of North Dakota, $1,750,000 received as an oil impact grant from the Department of Trust Lands, $2,207,000 in private fundraising, $393,000 in approved state 13-15 Challenge funds, and $888,267 in local funds generated from training activities and to proceed with the project contingent upon receipt or guarantee of all funds.

II. BSC requests authorization to refinance housing/auxiliary revenue bonds.
   1) Authorize issuance of not-to-exceed $4,000,000 State Board of Higher Education of the State of North Dakota, BSC Housing and Auxiliary Facilities Revenue Refunding Bonds, Series 2015, for the purpose of refinancing the outstanding BSC Housing and Auxiliary Facilities Revenue Bonds, Series 2005, maturing on and after May 1, 2016, and paying the costs of issuance of the Series 2015;
   2) Authorize the BSC President and/or Interim Executive Vice President to approve the sale of the bonds provided that the rate not exceed 4%, provided the present value of the debt service savings is not less than 2%. The approximate final date upon which the principal amount of the obligation will mature or become payable is May 2030;
   3) Appoint the firm of Arntson Stewart Wegner PC as the bond counsel and Public Financial Management, Inc. as the financial advisor.

III. Authorize an inter-funding borrowing, and related planned fund deficit, of $500,000 for the purchase and installation of an electronic scoreboard for the MisU Dome.

IV. Authorize funding source change for the construction by Valley City Parks and Recreation of a Health, Wellness and Physical Education Building, located on the VCSU campus from $15 million in private and $1 million in State Challenge Grant (up) to $13 million private, $1 million State Challenge Grant and $2 million student fee revenues; seek appropriate legislative authorization; and, further authorize an increase in the Fitness Facility fee from $0.42 per credit hour up to $12 per credit hour by no later than Fall 2017.

20. Other Board Consent

I. Authorize UND to proceed with various classroom and laboratory upgrade projects for the College of Engineering and Mines (CEM) at an estimated cost of $1,375,000 to be funded from local funds. Authorize NDSU to proceed with the Music Building South Entry Renovation project at an estimated cost of $350,000 funded from appropriated operations funding.

II. Authorize DSU to proceed with replacement of the waste water risers in Pulver Hall at an estimated cost of $566,195 to be paid from local auxiliary funds.

III. Authorize NDSU to proceed with the Music Building South Entry Renovation project at an estimated cost of $350,000 funded from appropriated operations funding.

Board Policy

First Reading
21. Policy 903 – Sales or Removal of Buildings

Second Reading
22. None
Policies Under Review

- Policy 340.2 – Foundations
- Policy 918 – Alcoholic Beverages on Campus
- Policy 611.10 – Employee Responsibility and Activities: Theft, Fraud, Abuse and Waste
- Policy 840 – Contract Review

Adjourn

Future Board Meetings

- February 26, 2015 – BSC
- March 26, 2015 – BSC

Contact Kristie Hetzler (701) 328-2966 or kristie.hetzler@ndus.edu prior to the scheduled meeting date if auxiliary aids or services are needed.
The following draft minutes have not yet been approved by the SBHE
North Dakota State Board of Higher Education
Minutes of the November 20, 2014, Meeting
North Dakota State University, Fargo

An Association of Governing Board consultant, Dr. Tom Meredith, conducted Board training from 8:05 a.m. to 10:30 a.m. CT., on the following topics:
- Board Governance
- Fiduciary Duties
- Self-Assessment
- Board Agenda Structure
- Future Challenges
- Internal and External Relationships

Break from 10:30 a.m. CT to 10:45 a.m. CT.

Board Chair Diederich called the meeting to order at 10:45 a.m. CT.

Members present:
- Dr. Kirsten Diederich, Board Chair
- Mr. Grant Shaft
- Ms. Kari Reichert
- Dr. Eric Murphy, Faculty Adviser
- Dr. Kevin Melicher
- Dr. Terry Hjelmstad, Vice Chair
- Mr. Chris McEwen
- Ms. Janice Hoffarth, Staff Adviser
- Ms. Kathleen Neset
- Mr. Don Morton

Interim Chancellor present: Dr. Larry C. Skogen

Institution Presidents present:
- Dr. Ken Grosz, Dean, DCB
- Dr. Doug Darling, President, LRSC
- Dr. Gary Hagen, President, MaSU
- Dr. John Richman, President, NDSCS
- Dr. Dean Bresciani, NDSU
- Dr. Robert Kelley, President, UND
- Dr. Margaret Dahlberg, Interim President, VCSU
- Mr. Drake Carter, Provost/VP for Academic & Student Affairs, BSC
- Dr. Steve Shirley, President, MiSU
- Dr. Raymond Nadolny, President, WSC
- Dr. D. C. Coston, President, DSU

NDUS senior staff present:
- Dr. Sonia Cowen, Interim Vice Chancellor for Academic and Student Affairs
- Ms. Linda Donlin, Director of Communications and Media Relations
- Ms. Cynthia Goulet, General Counsel
Approval of Board Agenda
Melicher moved, McEwen seconded, to approve agenda with the addition of the following items to be discussed:
• Chancellor search timeline
• Committee structure

Neset, Shaft, Hjelmstad, Melicher, McEwen, Morton, Reichert, and Diederich voted yes. The motion carried.

Approval of Minutes
McEwen moved, Morton seconded, to approve the following Board meeting minutes:
• October 2, 2014
• October 30, 2014
• November 6, 2014

Melicher, Neset, Hjelmstad, McEwen, Diederich, Shaft, Reichert, and Morton voted yes. The motion carried.

Admissions Standards
Dr. Sonia Cowen reviewed the revised recommendations of the Admissions Taskforce.

The Taskforce recommended the following general undergraduate admissions index for UND and NDSU, effective fall of 2016:

1. Admit first-time, full-time college students who have a minimum composite ACT score of 22 and minimal cumulative high school GPA of 2.75.
2. Enable NDSU and UND to admit first-time, full-time college students who have ACT scores and/or cumulative high school GPAs below this standard if they demonstrate potential to succeed academically, based on other factors.
3. Require that first-time, full-time college students who have graduated from North Dakota high schools, who are under the age of 25 on the first day of class, and who seek admission:
   a. In the fall of 2016, have completed successfully a minimum of 13 courses of this State’s high school core curriculum;
   b. In the fall of 2017, have completed successfully a minimum of 14 courses of this State’s high school core curriculum; and
   c. In the fall of 2018 and thereafter, have completed successfully a minimum of 15 courses of this State’s high school core curriculum.

The Task Force recommended the following general undergraduate admissions index for NDUS regional universities and MiSU, effective fall of 2016, for first-time, full-time college students: as proposed to the SBHE on June 26, 2014.

The Task Force further recommended the SBHE monitor the impact of increased admissions standards on enrollment.
Melicher moved, McEwen seconded, to approve the recommended admission standards.

Melicher, Neset, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

Board Member Ms. Kathleen Neset departed the meeting at 11:30 a.m. CT.

**High Performance Computing**

Dr. Josh Riedy and Dr. Tom DiLorenzo explained the benefits of high performance computing for the State and NDUS. A collaborative center for computation and data could achieve national leadership in advanced computational research and development through the exploitation of two major opportunities. First, having new, highly capable systems would enable recruiting and sustaining of the other leadership component: talent/expertise. The second major reason is that truly collaborative, academic–industry partnerships in advanced computational research are still relatively new; there are few true leaders in this context. North Dakota would leverage its current competitive positions in petroleum, agriculture, and aviation to create new computational programs focused on collaboration and technology transfer, while using new computing capabilities and expertise to create and grow programs in medicine, healthcare and big data analytics, which is increasingly important across all industry, education, and public policy sectors.

McEwen moved, Shaft seconded, to support hosting enhanced high performance computing resources in the form of a collaborative center for computation and data intended to serve the State, including all North Dakota universities and companies choosing to participate. Furthermore, the SBHE requests inclusion of such resources in the Governor’s Executive Budget similar to that of the Northern Tier Network.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

**Approve Draft Legislation**

Interim Chancellor Skogen discussed bills that may be pre-filed for the 2015 legislative session:

Open records
- Exempting 360 personnel reviews of the presidents
- Exempting the working papers of the NDUS chief auditor

Grants
- Increasing the individual grants in the student financial assistance program from $1600 to $2000 per recipient per academic year

Facilities
- Approval of the Woods Hall renovation project at DSU
- Purchase of additional land for the Dickinson Research Extension Center
- Clearly defining maintenance work so that the NDUS would not have to retain an architect/engineer for certain maintenance projects (e.g., $120,000 painting project)
- Streamlining the demolition process on certain buildings (e.g., old barn or shed)

Dr. Skogen noted that the bills would not be pre-filed if individual legislators intend to submit bills that would address these issues.
Melicher moved, McEwen seconded, to authorize the Chancellor, after consulting with the Chair of the State Board of Higher Education, to pre-file appropriate bills with the Legislative Council.

Shaft, Hjelmstad, Melicher, McEwen, Morton, Reichert and Diederich voted yes. The motion carried.

**SBHE Meeting December 18, 2014**
Chair Diederich stated that a few Board members will be out of the country on December 18th, 2014. She recommended the meeting be cancelled.

Shaft moved, Morton seconded, to cancel the December 18, 2018, Board meeting.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

**Special Board Meeting December 9, 2014**
Chair Diederich proposed a special Board meeting on December 9, 2014, to focus on the chancellor search timeline and process.

Shaft moved, Morton seconded, to approve a special Board meeting on December 9, 2014.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

**SBHE Academic and Student Affairs Committee**
Chair Reichert stated the SBHE Academic and Student Affairs Committee recommended approval of the following tenure requests:

- North Dakota State University
  - Michael James Yellow Bird, Ph.D., Professor of Sociology and Anthropology, Department of Sociology and Anthropology, College of Arts, Humanities and Social Sciences.

- The University of North Dakota
  - Malak Kotb, Ph.D., Professor of Basic Sciences, Department of Medicine and Health Sciences;
  - Ralph Renger, Ph.D., Professor of Family and Community Medicine, Family and Community Medicine, School of Medicine and Health Sciences;
  - Gayle Roux, Ph.D., Professor of Graduate Nursing, Department of Graduate Nursing, College of Nursing and Professional Disciplines;
  - Larry Williams, Ph.D., Professor of Psychology, Department of Psychology, College of Arts and Sciences; and,
  - Margaret Williams, Ph.D., Professor of Management, Department of Management, College of Business and Public Administration.

Hjelmstad moved, McEwen seconded, to approve the SBHE Academic and Student Affairs Committee tenure recommendations.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

**NDSU Finance Revenue Bonds**
McEwen moved, Melicher seconded, to approve the following NDSU requests authorization to refinance housing/auxiliary revenue bonds:

1. Authorize issuance of not-to-exceed $24,000,000 State Board of Higher Education of the State of North Dakota, NDSU Housing and Auxiliary Facilities Revenue Refunding Bonds, Series 2015A, for the purpose of refinancing the outstanding NDSU Housing and Auxiliary Facilities Revenue Bonds, Series 2005, Series 2006A and Series 2006B Bonds, maturing on and after April 1, 2015, and paying the costs of issuance of the Series 2015A;

2. Authorize the NDSU President and Vice President for Finance and Administration to approve the sale of the bonds (Series 2015A) provided that the rate not exceed 5% and provided the present value of the debt service savings is not less than 3%. The approximate final date upon which the principal amount of the obligation will mature or become payable is April 1, 2036; and

3. Appoint the firm of Arntson Stewart Wegner PC as the bond counsel and Fieldman, Rolapp & Associates (Independent Financial Advisors to Government) as the financial advisor.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

Interim Chancellor’s Report
In November, the Higher Learning Commission notified Interim Chancellor Skogen that it is requiring an interim report (no later than September 1, 2015) and a focused visit (no later than November 29, 2015). Interim Chancellor Skogen called the HLC for clarification and was informed that it is expecting a single interim report from the system and will be conducting a single visit to the system office similar to the visit in April 2014. As anticipated, the report and focus visit will only focus on Criterion Five, Core Component 5.D.

Dr. Skogen updated the Board regarding the DSU Foundation’s financial situation. The university system office, DSU, and the ND Attorney General’s office are cooperating to address the issues. Dr. Skogen will continue to keep the Board apprised on this matter.

Counsel of College Faculties (CCF) Report
Mr. Fernando Quijano indicated the CCF will be holding their annual face-to-face meeting January 29, 2015, in Bismarck.

Staff Senate Report
Ms. Emma Tufte stated the staff senate is currently taking nominations for staff advisor to the State Board of Higher Education. The elections will be held in January 2015.

North Dakota Student Association (NDSA) Report
Mr. Conner Swanson informed the Board that he is resigning his position as President of the NDSA, effective fall 2015. He has taken a position at the State legislature. Mr. Zachary Niebuhr will be the next NDSA president and a new vice president will be elected. Mr. Connor stated that Kelsey Klein will be the NDSA lobbyist for the upcoming session.

Public Comment
Senator Connie Triplett, Grand Forks, stated she was pleased to hear the Board’s desire to improve communication with legislators. However, Senator Triplett expressed areas of concerns she would like the Board to consider for future discussion. She stated faculty pay is extremely low and there is not a clear definition of what it means to be a research institution, and she would like the Board to reconsider its policy that gives the presidents of the institutions full authority to run the campuses.

**Board Policy**
The following policies were considered for second reading and final adoption:

McEwen moved, Morton seconded, to approve SBHE [Policy 805.3](#), Application Fees.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

McEwen moved, Melicher seconded, to approve SBHE [Policy 611.2](#), Intellectual Property.

Shaft, Melicher, Hjelmstad, McEwen, Diederich, Reichert and Morton voted yes. The motion carried.

McEwen moved, Hjelmstad seconded, to approve SBHE [Policy 1912](#), Record Retention.

Melicher, Hjelmstad, McEwen, Diederich, Shaft, Reichert and Morton voted yes. The motion carried.

Melicher moved, Hjelmstad seconded, to approve the [HR Policy 23.2](#), Resignation.

McEwen, Diederich, Melicher, Hjelmstad, Shaft, Reichert and Morton voted yes. The motion carried.

Shaft motioned to adjourn.

Adjourned at 1:55 p.m. CT
The following draft minutes have not yet been approved by the SBHE
North Dakota State Board of Higher Education
Minutes of the December 9, 2014, Meeting
At Bismarck State College

Board Chair Diederich called the meeting to order at 11:15 a.m. CT.

Members present:

Dr. Kirsten Diederich, Board Chair
Mr. Grant Shaft
Ms. Kari Reichert
Dr. Eric Murphy, Faculty Adviser
Dr. Kevin Melicher

Dr. Terry Hjelmstad, Vice Chair
Mr. Chris McEwen
Ms. Janice Hoffarth, Staff Adviser
Ms. Kathleen Neset
Mr. Don Morton

Interim Chancellor present: Dr. Larry C. Skogen

Institution Presidents present:

Dr. Ken Grosz, Dean, DCB
Dr. Doug Darling, President, LRSC
Dr. Gary Hagen, President, MaSU
Dr. Dean Bresciani, President, NDSU
Dr. Robert Kelley, President, UND
Mr. Dave Clark, Interim President, BSC
Dr. Steve Shirley, President, MiSU

NDUS senior staff present:

Dr. Sonia Cowen, Interim Vice Chancellor for Academic and Student Affairs
Mr. Murray Sagsveen, Chief of Staff and Director of Legal Services
Ms. Linda Donlin, Director of Communications and Media Relations
Ms. Cynthia Goulet, General Counsel
Mr. Rick Tonder, Director of Facilities Planning
Ms. Kristie Hetzler, Executive Assistant to the State Board of Higher Education
Ms. Terry Meyer, Administrative Support Manager

Board Chair Diederich explained that N.D.C.C. section 44-04-20(6) provides that the Board, in a special meeting, may only consider the agenda items stated in the notice of the special meeting.

Approval of Agenda
Shaft moved, Nest seconded, to approve the SBHE meeting agenda.

McEwen, Reichert, Melicher, Morton, Shaft, Hjelmstad, Neset and Diederich voted yes. The motion carried.
SBHE Budget and Finance Committee

SBHE Budget and Finance Committee Chair, Mr. Morton, recommended approval for the following:

1. Authorize NDSU Dickinson Research Center (DREC) to enter into an exclusive option to purchase land agreement with the estate of Duane J. Boehm for 1,680 acres, with the purchase contingent upon the sale of 240 acres of existing DREC land. Proceeds of the sale to be used for purchasing the Boehm property, complete any required improvements, and fund any future increase in operating costs. Further, request authorization to seek legislative authority for the purchase, sale, and any required improvements through legislation introduced and sponsored by Senator Wardner, Dickinson.


3. Authorize WSC to borrow up to $300,000 from the WSC Foundation (at 2% annual interest for a five-year term) to partially fund the replacement of the new boiler plant serving Steven's Hall and the Fieldhouse.

4. Allocate $34,143 from 2013-2015 capital projects contingency pool to DCB for the campus generator.

5. Approve change in authorization for MiSU football stadium press box from $4.0 million to $5.0 million, funded $4 million from City of Minot and up to $1 million in MiSU local funds. Further, seek appropriate legislative authorization for the change.

Melicher requested separate consideration of item 3. Shaft moved, Melicher seconded, to approve one, two, four, and five of the SBHE Budget and Finance Committee recommendations.

Melicher, Morton, Shaft, Hjelmstad, McEwen, Reichert, Neset and Diederich voted yes. The motion carried.

Williston State College Boiler

Williston State College requested approval to borrow up to $300,000 from the WSC Foundation (at 2% annual interest for a five-year term) to partially fund the replacement of the new boiler plant serving Steven's Hall and the Fieldhouse.

Melicher suggested that “provided WSC Foundation does not use permanently restricted funds for the loan” be added to the motion. Shaft moved, Neset seconded, to approve the following motion:

Authorize WSC to borrow up to $300,000 from the WSC Foundation (at 2% annual interest for a five-year term) to partially fund the replacement of the new boiler plant serving Steven's Hall and the Fieldhouse, provided WSC Foundation does not use permanently restricted funds for the loan.

Hjelmstad, McEwen, Reichert, Melicher, Shaft, Morton, Neset and Diederich voted yes. The motion carried.

Board Consent:

1. Approve the Joint Powers Agreement between the State Board of Higher Education, on behalf of Valley City State University, and the Valley City Parks and Recreation District for the construction, management, and operation of the Valley City Health, Wellness & Physical Education Center on the VCSU campus.

2. Authorize NDSU to proceed with the Administration Building (Old Main) – Tuckpointing and Rewindow Projects at an estimated cost of $600,000 funded from June 30, 2014, reported capital project designated reserves per SBHE policy 810.1.
3. Authorize NDSU to proceed with the Ehly Hall Renovation Project at an estimated cost of $2,450,000 funded from June 30, 2014, reported capital project designated reserves per SBHE policy 810.1.

Shaft moved, Hjelmstad seconded, to approve the three board consent items.

Melicher, Shaft, Hjelmstad, McEwen, Morton, Reichert, Neset and Diederich voted yes. The motion carried

Chancellor Search

Interim Chancellor Skogen introduced the Chancellor Search Advisory Team and thanked them for their participation. The advisory members present were:

Dr. Russ McDonald, President, United Tribes Technical College  
Msgr. James Shea, President, University of Mary  
Dr. Kirsten Baelser, Superintendent, Department of Public Instruction  
Mr. Jon Backes, Attorney, McGee, Hankaia & Backes, PC  
Mr. Terry Olson, Executive Director, Williston State College Foundation  
Mr. Bruce Dolezal, Regional President, American Bank Center  
Mr. Perry Miller, Owner, Miller, Perry & Denise-Lochmor Apartments  
Mr. Andy Peterson, President & CEO, ND Chamber of Commerce

Ms. Cynthia Wagner Goulet explained that both the North Dakota Constitution and state law provide that all meetings of governmental bodies and of organizations or agencies supported in whole or in part by public funds, or expending public funds, are open to the public, unless otherwise specifically provided by law. Accordingly, meetings held by the Board, including meetings involving the appointment of a chancellor, are subject to the open meetings laws. This meeting, held in connection with the chancellor search process, is a "special" meetings as that term defined by state laws. Ms. Goulet stated that if any subcommittees are assigned, including the current advisory team for the chancellor search, the open meetings laws would apply to them as well. Discussions do not have to be face-to-face to trigger open meetings requirements. Discussions occurring by telephone, videoconference, or by email communications are considered meetings, and must comply with open meetings requirements, if they involve a quorum of the Board or a committee and concern public business. Serial meetings are subject to open meetings laws. Open meetings requirements cannot be circumvented by "serial meetings." Serial meetings are multiple meetings (in person, by phone or by email) among small numbers of Board (or committee) members regarding the same topic. If the total number of members involved in the discussions constitutes a quorum, the serial meetings must comply with open meetings requirements.

Charge to State Board of Higher Education

Chair Diederich explained the search for the next Chancellor of the North Dakota University System has begun and is expected to conclude mid-May. She asked that each commit to the following timeline and search expectations:

- Attend search meetings – it is anticipated that the Board and Advisory Team will meet four times in addition to the May 14, 2015, SBHE meeting, where the SBHE will select the next Chancellor.
- Participate in listening meetings and discussions that identify priorities and personal and professional attributes sought in the next Chancellor and incorporated into the search profile.
- Review all candidate applications and identify a short list of candidates for additional screening and consideration.
- Participate in interviews of top candidates, then identify semifinalists.
• Assist with interview visits – as needed; identify list of finalists.
• Interview finalists and select next Chancellor.

Break (11:45 a.m. – 12:15 p.m. CT)

Board Chair Diederich called the meeting to back to order at 12:20 p.m. CT.

**Chancellor Search Listening Sessions**
The Board members reported they received good input from stakeholders across the state at the chancellor search listening sessions they conducted at the various institutions. They indicated there will be more listening sessions in the upcoming days. If the public can’t make it to one of the sessions, they may send comments to Chancellor.search@ndus.edu.

**Roles and Responsibilities**
Interim Chancellor Skogen reviewed a draft roles and responsibilities report. He stated the report is only a draft; however, he would like input from the Board on the reporting structure for the presidents before the Roles and Responsibilities Task Force meets again. Board members were in agreement to keep the current reporting structure. The presidents report to the Chancellor, however, the Board has the authority to hire and fire Presidents.

**Association of Governing Boards (AGB)**
Dr. McCormick and Ms. Fitzgerald, Association of Governing Boards (AGB), explained that the first step in the search process is to publish a detailed ad indicating what the needs and expectations of the next Chancellor are. Dr. McCormick stated, in order to stay on the timeline, the advertisement should go out by January 15, 2015, including posting it to the Chronicle of Higher Education. The consultants will consider the broad input on desired characteristics for the next Chancellor from the Board members, listening sessions held at the institutions, presidents, advisory group, and feedback and comments received by email. After consultation with the various groups the consultants will deliver a draft advertisement and profile to chair for final approval. The consultants will create a website for applications, actively recruit candidates, and receive inquiries/applications/nominations. The application deadline is March 17, 2015.

Melicher moved, Hjelmstad seconded, to delegate authority to Chair Diederich, Chancellor Skogen, and a representative of the Chancellors Cabinet to work with consultants to finalize the chancellor search profile.

Melicher, Hjelmstad, McEwen, Morton, and Diederich voted yes. Reichert, Neset, and Shaft voted no. The motion carried.

**Timeline**
Ms. Terry Meyer has worked with the AGB consultants and the Board Chair to develop the following timeline:

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/6/14</td>
<td>SBHE approved RFP to seek consultant for search, and assumed all responsibility for search related functions (in lieu of creating a committee therefore).</td>
</tr>
<tr>
<td>11/7/14</td>
<td>Published RFP for search consultant</td>
</tr>
<tr>
<td>11/21/14</td>
<td>Due date for consultants to submit a proposal</td>
</tr>
<tr>
<td>11/24-26/14</td>
<td>Chancellor evaluated consultants and selected one</td>
</tr>
<tr>
<td>12/9/14</td>
<td><strong>First Meeting</strong></td>
</tr>
<tr>
<td>Date Range</td>
<td>Event</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| No later than 1/8/15 | Consultants deliver draft advertisement and profile to Chair for final approval  
Consultants/Chair, Chancellor Cabinet representative finalize draft advertisement  
SBHE will receive approved copy of advertisement and profile |
| 12/9/14-1/15/15 | NDUS Office develops website presence for search |
| 1/15/15 | Chancellor search is launched with approved electronic posting  
(Approved reduced, block advertisement for *Chronicle of Higher Education* submitted Jan. 19, 2015)  
Approved advertisement posted with application deadline 3/17/15  
Advertisement and Profile placed on Consultant’s website |
| 1/15/15-3/17/15 | Consultants actively recruit candidates  
Consultants receive inquiries/applications/nominations  
Consultant creates website for all applications  
*Chronicle of Higher Education* advertisement, Jan. 30, 2015 edition |
| 3/17/15 | Application deadline for best consideration |
| 3/20/15 | Applications released to SBHE for review |
| 3/26/15 | **Second Meeting**  
Consultants in-person with SBHE  
SBHE meets to identify top candidates for IVN interviews  
Consultants provide draft interview questions for consideration, as requested |
| Following 3/26/15 meeting | Consultants contact top candidates, re: interview process for IVN interviews, April 14; dates given for on-campus meetings/interview with SBHE in the event they are selected for semifinalist/finalist interviews  
Consultants conduct reference checks on top candidates |
| 4/14/15 | **Third Meeting**  
Consultants available by telephone  
SBHE interviews top candidates via IVN  
Consultants deliver report on reference checks  
SBHE narrows list to semifinalists |
| Following 4/14/15 meeting | Consultants contact semifinalists and candidates not selected  
Consultants conduct off-list reference checks  
Consultants provide draft interview questions, as requested |
| 4/28-30/15 | **Fourth Meeting**  
SBHE/Advisors to meet 4/30/15  
Consultants in-person with SBHE  
Semifinalists meet with broad-based internal and external |
<table>
<thead>
<tr>
<th>Constituencies</th>
<th>4/30/15</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SBHE hears/considers off-list reference check information</td>
<td>Consultants contact finalists and semifinalists not selected</td>
</tr>
<tr>
<td>• SBHE narrows list to final candidates for further consideration</td>
<td>Consultant requests background checks with approval of finalists; report delivered to Chair (or designee)</td>
</tr>
<tr>
<td></td>
<td>Consultants provide interview questions, as requested</td>
</tr>
<tr>
<td></td>
<td>Site visit to final candidates’ home institution by a team of board members</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5/14/15</th>
<th>\</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SBHE meets and interviews finalists</td>
<td>SBHE appoints next chancellor of NDUS</td>
</tr>
<tr>
<td>• Chair (or designee) receives background check reports from AGB Search Consultants</td>
<td>\</td>
</tr>
<tr>
<td>• Offer extended to successful candidate</td>
<td>\</td>
</tr>
<tr>
<td>• Consultants assist NDUS Office with communication plan/announcement, as requested</td>
<td>\</td>
</tr>
<tr>
<td>• Consultants assist with transition plan, as requested</td>
<td>\</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5/14/15</th>
<th>\</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consultants assist NDUS Office with communication plan/announcement, as requested</td>
<td>\</td>
</tr>
<tr>
<td>• Consultants assist with transition plan, as requested</td>
<td>\</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>On 7/1/15</th>
<th>\</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Next Chancellor assumes office</td>
<td>\</td>
</tr>
<tr>
<td>• Consultants remain available to NDUS for one year following appointment</td>
<td>\</td>
</tr>
</tbody>
</table>

Melicher moved, Shaft seconded, to approve the timeline and process, which includes establishing future meeting dates.

Melicher, Morton, Shaft, Hjelmstad, McEwen, Reichert, Neset and Diederich voted yes. The motion carried.

**Communications Plan**
Ms. Fitzgerald explained that various national advertising strategies, using print and online media, will be utilized. They will be reaching out to a broad network for nominations and applications and a press release will be sent to necessary outlets.

Melicher moved to adjourn.

Meeting adjourned at 3:10 p.m. CT.
Vulnerability Assessment
Document ID: NDUS.docx
December 31, 2014
## Table of Contents

1. Executive Summary ................................................................................................................ 3
2. Introduction and Background ............................................................................................... 5
3. Scope......................................................................................................................................... 7
4. Methodology ............................................................................................................................ 8
5. Network Assessment Findings ............................................................................................... 9
   5.1. Finding 1 – Unsupported Operating Systems ................................................................. 9
   5.2. Finding 2 – Missing Software Patch or Required Upgrade ........................................ 10
   5.3. Finding 3 – Easily Guessed or Default Credentials .................................................. 11
   5.4. Finding 4 – Unsupported Web Server ......................................................................... 12
6. Internal Network Assessment .............................................................................................. 13
   6.1. Finding 5 – Systems with well-known exploits ............................................................ 13
      6.1.1. Heartbleed ............................................................................................................. 13
      6.1.2. Shellshock ............................................................................................................. 13
      6.1.3. IPMI Cipher Suite Zero ........................................................................................ 14
7. External Network Assessment ............................................................................................. 15
   7.1. Finding 6: Publicly Accessible Web Applications ....................................................... 15
   7.2. Finding 7: Firewall / NAT .............................................................................................. 15
8. Web Application Assessment Findings ............................................................................... 16
   8.1. Finding 8: Cross-Site Scripting ..................................................................................... 16
   8.2. Finding 9: Cleartext Password ...................................................................................... 17
   8.3. Finding 10: Session Token in URL .............................................................................. 17
   8.4. Finding 11: SQL injection ............................................................................................ 18
   8.5. Finding 12: Serialized Object in HTTP message .......................................................... 18
9. Conclusion ............................................................................................................................. 20
10. Points of Contact for this Report........................................................................................... 21
11. Appendix A: NDUS Response .............................................................................................. 22
List of Exhibits

Exhibit 1. Team Kimball’s Network Penetration Testing Methodology .............................................. 8
1. Executive Summary

Information technology (IT) security practices are critically important for the North Dakota University System and its institutions to protect large amounts of sensitive and confidential information that are stored on their computer systems, including information for more than 47,000 students and 11,000 faculty and staff. Universities are attractive targets for computer hackers because they traditionally have a strong culture of academic freedom that values open access to information and a free exchange of ideas. By providing numerous computer labs and high-capacity internet access that allows for the exchange of information at high speeds, universities not only accommodate their many users, but also create an attractive target for computer hacking. University IT security problems are occurring more often through weaknesses in network and web-based computer programs and (applications) as well as via social engineering techniques.

On behalf of the North Dakota State Auditor and the North Dakota University System, from October 1 to October 31, 2014, Team Kimball (the team) carried out external and internal vulnerability assessments on the networks associated with the North Dakota University System (NDUS). These networks consisted of the following campuses as well as NDUS networks in the listed locations: Bismarck State College (BSC), Dakota College at Bottineau (DCB), Dickinson State University (DSU), Lake Region State College (LRSC), Mayville State University (MASU), Minot State University (MISU), North Dakota State College of Science (NDSCS), North Dakota State University (NDSU), NDUS Offices (Fargo, Bismarck, Grand Forks), University of North Dakota (UND), Valley City State University (VCSU), Williston State College (WSC)

External assessments were conducted with no privileges in order to mimic anyone surfing the Internet. External network access as well as externally facing web applications were evaluated for each of the campuses. The majority of internal assessments were conducted with the same access and privilege level a student or a member of the faculty would have within the university system. In some cases as part of the internal assessment Team Kimball was provided with additional access to reach internal network components for evaluation. The scans were configured to check for vulnerabilities on any host that was controlled by the campus. Vulnerabilities were identified but no exploitation of the vulnerabilities that were detected was attempted. Access to certain systems was however obtained due to default login credentials being utilized.

Key findings at each of the campuses can be summarized into the following twelve categories. Each of the findings is provided in more detail within this report.

1. Unsupported Operating Systems
2. Missing software patch or required software upgrade
3. Easily guessed or Default Credentials
4. Unsupported Web Server
5. Well Known Exploits
6. Publicly Accessible Web Applications
7. Lack of Firewall / NAT
8. Cross-site Scripting
9. Cleartext submission of Password
10. Session Token in URL
11. SQL Injection
12. Serialized Object in HTTP message

All found vulnerabilities were rated on a scale from Critical to Low based on the common vulnerability scoring system (CVSS). Details associated with each of the findings as well as remediation guidance were provided to NDUS and to each of the campuses. The 12 findings listed above were all considered Critical or High. Appendix A of this document contains a response from NDUS to the findings of the vulnerability assessment.
2. Introduction and Background

Information technology (IT) security practices are critically important for the North Dakota University System and its institutions to protect large amounts of sensitive and confidential information that are stored on their computer systems, including information for more than 47,000 students and 11,000 faculty and staff. Universities are attractive targets for computer hackers because they traditionally have a strong culture of academic freedom that values open access to information and a free exchange of ideas. By providing numerous computer labs and high-capacity internet access that allows for the exchange of information at high speeds, universities not only accommodate their many users, but also create an attractive target for computer hacking. University IT security problems are occurring more often through weaknesses in network and web-based computer programs and (applications) as well as via social engineering techniques.

IT security violations have occurred both in North Dakota and other states. For example:

- In February, 2014 an NDUS IT system was inappropriately accessed, which could have exposed the personal information of more than 290,000 current and past students and employees. Officials learned that unauthorized access was initially gained in October 2013. An investigation involving law enforcement and an outside forensics group revealed that the unauthorized party – thought to be based outside of the U.S. – was likely not going after the data, but instead was leveraging the processing power of the server to attack other computers and systems, according to the NDUS website.

- In August, 2014 eight North Dakota State University employees had their paychecks stolen by online scammers. It happened during a payroll cycle when the employees fell victim to what’s known as a phishing scam, which involves emails pretending to be from official sources. “The email asked employees to click on a link and verify their information for payroll distribution, and eight employees responded,” NDUS said in a statement. “Unfortunately, those employees’ paychecks were then re-directed to the scammer’s account. They reported the incidents, which were then reported to authorities.” North Dakota State University covered about $20,600 in lost wages for employees who fell victim to this email scam according to a report presented to state lawmakers that included previously unreleased details about the so-called “spear phishing” attack.

- In September, 2014 North Dakota State College of Science Information Technology Services department had been alerted to malware activity on a number of NDSCS-owned computers in Wahpeton and Fargo and took immediate steps to ramp up security on its systems. Personal information such as names, Social Security numbers and mailing addresses of more than 15,000 current and former students and employees were contained on some of the affected computers. Those whose information was found were notified of the incident. After the malware was discovered, immediate action was taken to secure NDSCS systems. This included conducting a thorough internal investigation by NDSCS and North Dakota University System Information Technology experts. Law enforcement was contacted, and key systems were sent to a national forensic organization to confirm the analysis.
University breaches have been on the rise recently. The University of Maryland and Indiana University both recently announced incidents involving hundreds of thousands of victims, with the Maryland occurrence also being the result of an attack.

IT security is essential to help campuses comply with federal laws and regulations designed to protect sensitive information such as educational records, personally identifiable information, and financial aid records.

On behalf of the North Dakota State Auditor and the North Dakota University System, from October 1 to October 30, 2014, the team carried out external and internal vulnerability assessments on the networks associated with the North Dakota University System (NDUS). These networks consisted of the following campuses as well as NDUS networks: Bismarck State College (BSC), Dakota College at Bottineau (DCB), Dickinson State University (DSU), Lake Region State College (LRSC), Mayville State University (MASU), Minot State University (MISU), North Dakota State College of Science (NDSCS), North Dakota State University (NDSU), NDUS Offices (Fargo, Bismarck, Grand Forks), University of North Dakota (UND), Valley City State University (VCSU), Williston State College (WSC)

External assessments were conducted with no privileges in order to mimic anyone surfing the Internet. External network access as well as externally facing web applications were evaluated for each of the campuses. The majority of internal assessments were conducted with the same access and privilege level a student or a member of the faculty would have within the university system. In some cases as part of the internal assessment Team Kimball was provided with additional access to reach internal network components for evaluation. The scans were configured to check for vulnerabilities on any host that was controlled by the campus. Vulnerabilities were identified but no exploitation of the vulnerabilities that were detected was attempted. Access to certain systems was however obtained due to default login credentials being utilized.
3. Scope

Testing was performed on all networked devices within the ranges specified by each campus. External and Internal ranges were assessed. The scans checked for known vulnerabilities and weaknesses in the network and attached hosts and appliances. All relevant web applications were also audited using Burp Suite Professional vulnerability scanner. All detected vulnerabilities and weaknesses were documented, and guidelines for remediation were provided.
4. Methodology

The team performed an external and internal vulnerability assessment to determine which hosts were visible from outside of the NDUS and each of the institutions networks. The team followed the standard penetration test methodology for the security assessment but stopped at the point where the team would attempt to exploit the target systems. Exhibit 1 shows the methodology. The light blue boxes were completed as part of the assessment.

The team utilized the following tools to assess the network and networked devices:

- NESSUS (commercial version)
- Core Impact Pro
- BURP Suite Professional Vulnerability Scanner
- NMAP Network Scanner

Exhibit 1. Team Kimball’s Network Penetration Testing Methodology

The findings associated with each of the assessments: Internal, External, and Web Sites can be found in their respective sections.
5. Network Assessment Findings

The following findings represent a sanitized version of the vulnerability assessments that were presented to each of the NDUS campuses. Detailed assessment results as well as remediation for each of the findings has been provided to the campuses and many of them had resolved a significant portion of the critical items prior to the team leaving the site. This section contains findings that were common to both the external and internal network assessment. For the external assessment, the assessment team was connected to the internet with no special access. The majority of internal assessments were conducted with the same access and privilege level a student or a member of the faculty would have within the university system. In some cases as part of the internal assessment Team Kimball was provided with additional access to reach internal network components for evaluation. Four (4) findings are detailed in this section and these findings are representative of most of the colleges and universities that were assessed.

5.1. Finding 1 – Unsupported Operating Systems

The assessment team found unsupported operating systems at 10 of the 12 locations assessed. The operating systems ran the gambit from Windows, UNIX, MacOS, and Linux systems. The proliferation of unsupported and end-of-life products is an issue for many organizations and increases the effort required to minimize risk. As applications and operating systems reach their end-of-life (EOL), vendors stop offering support. Therefore, security and stability decrease, allowing attackers to exploit found vulnerabilities that will never receive a patch or security update. Patches, updates and security fixes will no longer be available, so identifying systems running EOL operating systems and applications is an important part of assessing and minimizing organizational risk.

End of Support for XP SP2 (x86) and Windows 2000

Windows 2000™ is no longer supported by Microsoft. Its mainstream and extended support ended on June 30, 2005, and July 13, 2010, respectively. The Service Pack support for the 32-bit edition of Windows XP™ SP2 was retired on July 13, 2010 and the 64-bit edition of XP SP2 was retired on April 8, 2014.

Consumers, business users, and software developers using Windows 2000™ and Windows XP™ SP2 (x86) will no longer receive updates for security fixes and non-security hotfixes.

The Risks in Using Unsupported Operating Systems

There are risks in using Windows 2000™ and XP SP2 (x86) because consumers will no longer receive product support, bug fixes, and patch releases. Any known and unknown vulnerabilities affecting the unsupported operating systems create a risk of exploitation or data breaches from attackers on the vulnerable OS.

Other risks from using Windows XP™ SP2 (x86) and Windows 2000™ occur whenever malware creators release malicious codes targeting unsupported and unpatched operating systems. Over time, the software developers and security software vendors offering protection for an unsupported OS will also stop providing detection signatures and product support. With that in mind, any malware targeting old OS puts an organization at risk of data loss or a security breach. The worst scenario is when critical and sensitive data is stolen by malware attackers.
In Secunia’s Half Year Report 2010, Apple OS is the top vendor with the most vulnerabilities. Oracle comes in second place, while Microsoft holds the third position. Other vendors in the list are HP, Adobe Systems, IBM, VMWare, Cisco, Google, and Mozilla. The report also states, "On average, 10 vendors are responsible for 38% of the vulnerabilities per year." This is a cause for concern because consumers have supported platforms or applications installed on the computers that depend on product support, security fixes, and non-security hotfixes to help protect the computer and data. The use of operating systems that are no longer supported will almost always provide attackers with the ability to exploit the targeted systems.¹

**Recommendations for Finding 1 - Unsupported Systems**

1. Where possible move from unsupported versions of operating systems to supported versions.
2. For systems where this is not possible or where the cost is too high, consider defense in depth strategies to mitigate risk to these systems:
   a. Shutdown ports and applications not required
   b. Limit access to the machine
   c. Segregate the machine where possible
3. The following operating systems should not be allowed within the NDUS network. If a system is required, a waiver should be provided and defense in depth strategy outlined for protection of the machine and the attached networks.²
   - Macintosh System Software (any version)
   - Mac OS 9 and below
   - Microsoft Windows XP Professional and below
   - All 16-bit Windows releases (Windows 98, Window 95 and Microsoft DOS)
   - Solaris 9 / SunOS 5.9 and below
   - AIX 6.1 and below
   - Debian 5.0.x and below
   - FreeBSD 6.x and below
   - Red Hat Enterprise Linux 2.1 and below
   - SUSE Linux Enterprise 11 and below
   - Ubuntu 13.10 and below (LTS version 12.04 is still supported)

**5.2. Finding 2 – Missing Software Patch or Required Upgrade**

It is imperative that software patches and software upgrades are applied in a timely manner, particularly those that are linked to application security. At the same time, it is important that the IT teams have sufficient time to evaluate the patches and upgrades to determine if their specific

---

mix of applications will potentially have issues with the upgrade. This also allows the IT staff to ensure that their customer base does not have an adverse reaction to the patch.

Patch Management is an important IT security practice designed to proactively prevent the exploitation of vulnerabilities on system devices. The expected result is to reduce the time and money spent dealing with vulnerabilities and their exploitation. Taking a proactive approach to patch management can reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after a vulnerability has been exploited.

This item was the largest finding in the assessment and contributed to the largest reported vulnerability. It is imperative that each of the campuses have a program in place to identify required patches and then to implement them in a timely manner. They must also have a system in place to prioritize those that may not be critical but are well known vulnerabilities that need to be addressed.

**Recommendations for Finding 2 – Missing Patches or Upgrades**

1. Ensure that all campuses are running Nessus or equivalent tools for vulnerability assessment. This will allow them to determine what patches are required and be in a better position to provide prioritization associated with patching.
2. All campuses must apply all applicable hardware, software, and applications patches in a reasonable timeframe based on the severity of the issue. NDUS and the campuses should define the severity of the issue based on their current policies and procedures and risk associated with the software.
   
   Typical Patch Timelines:
   - Critical – 1 week
   - High - 45 days
   - Medium/Low - up to 1 year
3. Ensure a patch management program is in place that is tracking systems that are affected and timeline to resolution.
4. NDUS and campuses should evaluate commercially available patch management products to expedite patching and updates. Some commercially available products include:
   
   **Commercially Available Patch Management Products:**
   - ManageEngine Desktop Central (Win/Mac/3rd)
   - Symantec Altiris (Win/Mac/Linux)
   - Dell Kace (Win/Mac/Linux/3rd)
   - GFI LanGuard (Win/Mac/Linux/3rd)

**5.3. Finding 3 – Easily Guessed or Default Credentials**

Passwords are instrumental in the protection of data, systems, and networks. For example, passwords are used to authenticate users of operating systems and applications such as email, labor reporting, and remote access. In addition, passwords are often used in less visible ways; for example, a biometric device may generate a password based on a fingerprint scan, and that password is then used for authentication.
Organizations should be aware of the drawbacks of using password-based authentication. There are many types of threats against passwords, and most of these threats can only be partially mitigated. Also, users are burdened with memorizing and managing an ever-increasing number of passwords. However, although the existing mechanisms for enterprise password management can somewhat alleviate this burden, they each have significant usability disadvantages and can also cause more serious security incidents because they permit access to many systems through a single authenticator. Therefore, organizations should make long-term plans for replacing or supplementing password-based authentication with stronger forms of authentication for resources with higher security needs.

During our assessment, every campus was found to have systems with easily guessed or default credentials. These systems are goldmines for hackers as this provides easy access to the campuses internal network and may allow a hacker to move around (pivot) and gain additional footholds within the organization at will. In addition, if they are able to gain access to administrator level accounts the attackers will have full access to the system and any files or network access associated with the account.

**Recommendations for Finding 3 – Easily Guessed or Default Credentials**

1. Create a password policy that specifies NDUS password management related requirements
2. Protect passwords from attacks that capture passwords (use HTTPS for web password submission or use multifactor authentication)
3. Configure password mechanisms to reduce the likelihood of successful password guessing and cracking
4. Determine requirements for password expiration based on balancing security and usability
5. Ensure systems are not deployed with default or out of the box user/password settings

**5.4. Finding 4 – Unsupported Web Server**

During the Assessment it was determined that five of the twelve campuses assessed had unsupported web servers operating in their networks. These represent a security issue based on the risk associated with discovered vulnerabilities that cannot be patched or remedied by the web server supplier. Since these applications are directly connectable via the internet, it is easy for an attacker to find these targets and exploit them.

**Recommendations for Finding #4: Unsupported Web Server**

1. Evaluate the need for the web server. If it is no longer being used shut it down.
2. Upgrade the server to a supported release.
3. If the server is no longer supported, look for a web server that is supported and will meet the requirements associated with your applications.
6. Internal Network Assessment

In addition to the above common findings, the following findings were unique to the internal network assessment:

6.1. Finding 5 – Systems with well-known exploits

While performing the internal assessment, nine out of the twelve campuses assessed contained systems with well-known exploits. Systems were found with Heartbleed, Shellshock, and IPMI Cipher Suite Zero exploits. Each of these exploits has been in the news and patches have been available for some time. In addition, Nessus and other vulnerability assessment tools have supported identification of each of these vulnerabilities. These are called out because each of these vulnerabilities is known to be exploitable. It is important to note that these vulnerabilities were only found internal to the campuses that were assessed, however, if an attacker is able to breach the outer perimeter and then finds additional easily accessible machines internal to the network, it is then very easy to setup multiple points of presence which will make removal from the network much more difficult to detect and accomplish.

6.1.1. Heartbleed

The Heartbleed bug tricks a server into spilling out extra information from its memory. A server's memory often includes sensitive personal information, such as your passwords, credit card numbers, and other data you wouldn't want anyone else to see or have access.

This information is usually encrypted, which means it’s translated to an indecipherable code when it's transferred between servers, but Heartbleed can decode this encryption and store the codes used to protect your data. Heartbleed takes advantage of a vulnerability in OpenSSL, a popular encryption standard used to power a giant chunk of the Web.

Heartbleed attacks a vulnerability in OpenSSL called Heartbeat, which is a means of calling out to a server to make sure the connection is secure. The Heartbeat message usually contains arbitrary data and length field denoting how many bytes of data are in the message. The server would then transmit that exact message back to the original sender to prove that the connection is secure. The Heartbleed bug involves an issue with the server reading the length field incorrectly, which in turn tricks your server into transmitting more data than it should without realizing it.

6.1.2. Shellshock

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.

Attackers exploited Shellshock within hours of the initial disclosure by creating botnets of compromised computers to perform distributed denial-of-service attacks and vulnerability scanning. Security companies recorded millions of attacks and probes related to the bug in the days following the disclosure.

Shellshock could potentially compromise millions of unpatched servers and other systems.
6.1.3. IPMI Cipher Suite Zero

“The Intelligent Platform Management Interface (IPMI) is a standardized computer system interface used by system administrators for out-of-band management of computer systems and monitoring of their operation. It is a way to manage a computer that may be powered off or otherwise unresponsive by using a network connection to the hardware rather than to an operating system or login shell.

Recommendations for Finding #5: Systems with Well-Known Exploits

1. Patch all systems that are found with these exploits with appropriate vendor-supported patch.
7. External Network Assessment

The following findings are unique to the external network assessment.

7.1. Finding 6: Publicly Accessible Web Applications

A number of publicly accessible web applications (not part of the campus web pages) were found to be externally accessible as part of the university network. Many of these applications were manually evaluated by Team Kimball and were found to be configured with default or easily guessed username and password for the administrator of the application. In addition, many of these systems had a web interface that should be disabled or blocked from external (public) access. Some of the applications were found to store and allow access to personally identifiable information (PII). Team Kimball was also able to send traffic to these applications, which could lead to denial of service and prevent the legitimate use of the applications by students and staff.

Recommendations for Finding #6: Publically Accessible Web Applications

1. Systems with web applications or appliances should be disabled if not required and should not be publicly accessible. If they need to be publicly accessible proper authentication mechanisms should be in place.

2. Ensure systems are not setup with default user or administrator credentials. These should be changed before deployment of the device.

7.2. Finding 7: Firewall / NAT

During the internal assessment it was noted that, four of the twelve campuses evaluated utilize public IP addresses for internal routing within the campus. In some cases, a bridged firewall is in place to provide routing rules and to provide application level filtering. Network Address Translation (NAT) allows a network to be protected by a single host (the router). The router acts as the gateway to the Internet, separating and protecting the hosts downstream from potential threats on the Internet. Due to the configuration of these 4 campuses their networks can be considered external. This means that hosts residing on this network can be accessed by anyone connected to the Internet; an attacker does not have to be on campus to access these hosts. It should also be noted that the usage of a firewall or NAT is not an end all be all solution. These measures should be implemented as part of a multi-faceted security approach.

Recommendation for Finding #7: Firewall/NAT:

1. Install and configure a routing firewall to provide NAT to these networks so they are no longer publicly facing.

2. Implement a multi-faceted security effort.
8. Web Application Assessment Findings

The website for each of the campuses and NDUS was assessed. The assessment team evaluated the web sites using Burp Suite Professional Vulnerability Scanner. This tool audits the web site for any potential attack vectors by issuing a number of requests and processing the results it receives from the server.

8.1. Finding 8: Cross-Site Scripting

During the web application assessment, nine of the twelve campus websites had cross-site scripting related issues.

Reflected cross-site scripting vulnerabilities arise when data is copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request which, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing the victim's session token or login credentials, performing arbitrary actions on the victim's behalf, and logging their keystrokes.

Users can be induced to issue the attacker's crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular web sites that allow content authoring, for example in blog comments. The attacker can create an innocuous looking web site which causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality which it contains, and the other applications which belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain which can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and therefore may be considered high risk. Similarly, if the organization which owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks, by injecting Trojan functionality into the vulnerable application, and exploiting users' trust in the organization in order to capture credentials for other applications which it owns. In many kinds of applications, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Recommendations for Finding #8: Cross-site Scripting

1. Input should be validated as strictly as possible on arrival, given the kind of content which it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-
defined regular expression. Input which fails the validation should be rejected, not sanitized.

2. User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including \(<\) " ' and \(=\), should be replaced with the corresponding HTML entities (\&lt; \&gt; \&quot; \&apos; \&amp; etc).

### 8.2. Finding 9: Cleartext Password

Passwords submitted over an unencrypted connection are vulnerable to capture by an attacker who is suitably positioned on the network. This includes any malicious party located on the user's own network, within their Internet Service Provider (ISP), within the ISP used by the application, and within the application's hosting infrastructure. Even if switched networks are employed at some of these locations, techniques exist to circumvent this defense and monitor the traffic passing through switches.

The application should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed. These areas of the application should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications. If HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over cleartext HTTP.

**Recommendations for Finding #9: Cleartext Password**

1. Replace HTTP web services with HTTPs version in instances where data must be protected.

2. Replace unsecured services, such as telnet and rlogin, with a secured SSH service. If you must operate unsecured command line services, it is recommended that you operate them within a secured tunnel like SSL/TLS or VPN.

3. Training for user awareness.

### 8.3. Finding 10: Session Token in URL

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referrer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

**Recommendations for Finding #10: Session Token in URL**

1. The application should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.
8.4. Finding 11: SQL injection

SQL injection vulnerabilities arise when user-controllable data is incorporated into SQL database queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

**Recommendations for Finding #11: SQL Injection**

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. The affected campuses should review the documentation for the database and application platforms to determine the appropriate APIs which can be used to perform parameterized queries. It is strongly recommended that the affected campuses parameterize every variable data item that is incorporated into database queries, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

Organizations should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective.

One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string in which it is inserted. However, if the data being incorporated into queries is numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped when initially inserted into the database is subsequently read from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data is reused, allowing the defense to be bypassed.

Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

8.5. Finding 12: Serialized Object in HTTP message

Our assessment identified that an application appears to submit a serialized object in a request parameter. This behavior can expose the application in various ways, including:

- Any sensitive data contained within the object can be viewed by the user.
- An attacker may be able to interfere with server-side logic by tampering with the contents of the object and re-serializing it.
An attacker may be able to cause unauthorized code execution on the server, by controlling the server-side function that is invoked when the object is processed.

Actual exploitation of any code execution vulnerabilities arising from the application's use of serialized objects will typically require the attacker to have access to the source code of the server-side application. This may mitigate the practical impact of this issue in many situations. However, it is still recommended to fix the underlying vulnerability.

**Recommendations for Finding #12: Serialized Object in HTTP Message**

1. The best way to avoid vulnerabilities that arise from the use of serialized objects is not to pass these in request parameters, or expose them in any other way to the client. Generally, it is possible to transmit application data in plain non-serialized form, and handle them with the same precautions that apply to all client-submitted data. If it is considered unavoidable to place serialized objects into request parameters, then it may be possible to prevent attacks by also placing a server-generated cryptographic signature of the object into the same request, and validating the signature before performing deserialization or other processing on the object.
9. Conclusion

Team Kimball identified vulnerabilities in the NDUS network and within the NDUS campuses networks. Vulnerabilities were identified in all networks that were evaluated as part of this report. Individual reports were provided to each of the campuses as well as the NDUS network. These reports provided detailed explanations associated with each of the vulnerabilities as well as recommended remediation guidance.

This report identified the common vulnerabilities that were presented in each of the campus reports for the NDUS as a whole. It identifies that there are 12 finding areas that need to be addressed and has provided recommendation guidance for addressing each of the findings. More specific and detailed guidance has been provided to each individual campus as part of their individual assessment.

Summary of recommendations:

- Training
  - Cybersecurity Awareness Training for NDUS personnel.
  - Specialized training for IT staff on best practices in information security and use of vulnerability scanning tools
- Deploy Defense-in-Depth strategies (multifaceted security)
- Patch/update process and automated patching where applicable
- Implement quarterly Social Engineering testing to baseline and track user awareness and response
- Expand vulnerability assessment to include penetration testing in order to validate the results and demonstrate the ramifications of the vulnerabilities.
10. Points of Contact for this Report

Program Manager – Team Kimball
   RD Porter
   Email: rd.porter@lrkimball.com
   Phone: 573-355-6881

Principal Architect - Enterprise Security & Protection
   Erik Wallace
   Email: ewallace@telecomsys.com
   Phone: 410-280-1184

Security Analysts - Enterprise Security & Protection
   Ryan Miller
   Brent Borton
   Kyle Jarrett
   Brian Lemons
   Phil Stoner
11. Appendix A: NDUS Response

NDUS Response to North Dakota University System Vulnerability Assessment dated 31 Dec 2014

Prepared by: Brad Miller, NDUS Director of Information Security

January 12, 2015
Finding 1 – Unsupported Operating Systems

Recommendations for Finding 1 - Unsupported Systems

4. Where possible move from unsupported versions of operating systems to supported versions.
5. For systems where this is not possible or where the cost is too high, consider defense in depth strategies to mitigate risk to these systems:
   a. Shutdown ports and applications not required
   b. Limit access to the machine
   c. Segregate the machine where possible
6. The following operating systems should not be allowed within the NDUS network. If a system is required, a waiver should be provided and defense in depth strategy outlined for protection of the machine and the attached networks.3
   - Macintosh System Software (any version)
   - Mac OS 9 and below
   - Microsoft Windows XP Professional and below
   - All 16-bit Windows releases (Windows 98, Window 95 and Microsoft DOS)
   - Solaris 9 / SunOS 5.9 and below
   - AIX 6.1 and below
   - Debian 5.0.x and below
   - FreeBSD 6.x and below
   - Red Hat Enterprise Linux 2.1 and below
   - SUSE Linux Enterprise 11 and below
   - Ubuntu 13.10 and below (LTS version 12.04 is still supported)

Response: Many of the systems identified in the assessment have already been either removed from the NDUS CTS and campus networks or have been migrated to a supported operating system. Some of the systems identified with unsupported operating systems are embedded in vendor hardware or appliances, and therefore cannot be easily removed or migrated without significant cost. These devices have been, or are in the process of being, secured with additional defense in depth techniques as mentioned in the recommendations until they can be updated or migrated. NDUS CTS and campuses will need to develop policy and procedures regarding methods of identifying systems with unsupported operating systems and actions to take when found.
Finding 2 – Missing Software Patch or Required Upgrade

Recommendations for Finding 2 – Missing Patches or Upgrades

1. Ensure that all campuses are running Nessus or equivalent tools for vulnerability assessment. This will allow them to determine what patches are required and be in a better position to provide.
2. All campuses must apply all applicable hardware, software, and applications patches in a reasonable timeframe based on the severity of the issue. NDUS CTS and the campuses should define the severity of the issue based on their current policies and procedures and risk associated with the software.
3. Ensure a patch management program is in place that is tracking systems that are affected and timeline to resolution.
4. NDUS and campuses should evaluate commercially available patch management products to expedite patching and updates.

Response: NDUS Core Technology Services (CTS) is currently using Nessus Enterprise to identify vulnerabilities on systems within key areas of the CTS network. The CTS Nessus Enterprise vulnerability scanning system has been made available to all NDUS campuses to use for ongoing scanning of their campus networks. Most of the campuses have accounts on the CTS Nessus system or have their own on-campus vulnerability scanning capabilities. Also, CTS and many of the NDUS campuses have and use commercial patch management systems. NDUS CTS and the campuses will need to develop vulnerability management and patching policies, procedures, and capabilities to ensure consistent and expedited patching of systems and applications.

Finding 3 – Easily Guessed or Default Credentials

Recommendations for Finding 3 – Easily Guessed or Default Credentials

1. Create a password policy that specifies NDUS password management related requirements
2. Protect passwords from attacks that capture passwords (use HTTPS for web password submission or use multifactor authentication)
3. Configure password mechanisms to reduce the likelihood of successful password guessing and cracking
4. Determine requirements for password expiration based on balancing security and usability
5. Ensure systems are not deployed with default or out of the box user/password settings

Response: Section 3.4 of NDUS Procedure 1901.2 Computer and Network Usage currently outlines password management requirements for NDUS CTS and campuses. These requirements currently address password length, complexity, secrecy, and default accounts. These requirements will be examined as part of an ongoing policy review, and any identified deficiencies or recommended changes will be addressed. All identified web password submissions not using HTTPS have been remediated. CTS is currently piloting a multifactor authentication solution for critical systems and applications.
Finding 4 – Unsupported Web Server

Recommendations for Finding #4: Unsupported Web Server
1. Evaluate the need for the web server. If it is no longer being used shut it down.
2. Upgrade the server to a supported release.
3. If the server is no longer supported, look for a web server that provides supports and will meet the requirements associated with your applications.

Response: Many of the unsupported web servers identified in the assessment have already been remediated. Ongoing Nessus vulnerability scans are needed to help identify any further, or future unsupported web servers, as well as other unsupported systems and applications, in order to secure, upgrade, or migrate them to a supported platform.

Finding 5 – Systems with well-known exploits

Recommendations for Finding #5: Systems with Well-Known Exploits
1. Patch all systems that are found with these exploits with appropriate vendor supported patch.

Response: Most of the well-known exploits categorized as critical or high on systems identified in this assessment have already been patched or remediated. NDUS CTS and the campuses will need to develop vulnerability management and patching policies, procedures, and capabilities to ensure consistent, expedited, and ongoing patching of systems and applications.

Finding 6: Publicly Accessible Web Applications

Recommendations for Finding #6: Publically Accessible Web Applications
1. Systems with web applications or appliances should be disabled if not required and should not be publicly accessible. If they need to be publicly accessible proper authentication mechanisms should be in place.
2. Ensure systems are not setup with default user or administrator credentials. These should be changed before deployment of the device.

Response: Efforts to evaluate and address publicly accessible systems and applications on NDUS and campus networks are currently underway. These publicly accessible systems do pose a significant risk. Policies, procedures, and capabilities will need to be developed by NDUS CTS and campuses to address the security of public-facing systems and web applications and determine whether or not they should be exposed to the external Internet. It will take considerable resources to remediate these issues due to the open network architecture at many of the campuses, the large number of systems currently on these networks, and the diverse population of faculty, staff, and students.
Finding 7: Firewall / NAT

Recommendation for Finding #7: Firewall/NAT:
1. Install and configure a routing firewall to provide NAT to these networks so they are no longer publicly facing.
2. Implement a multi-faceted security effort.

Response: NDUS CTS and many of the NDUS campus networks do currently use Network Address Translation (NAT) to create 'private' networks, but some of the campuses do not, and in some cases, this results in public facing systems that do not need to be. NDUS CTS and campuses will need to evaluate their environment and identify and implement firewalls, NAT, or other security mechanisms to protect their network and devices.

Finding 8: Cross Site Scripting

Recommendations for Finding #8: Cross Site Scripting
1. Input should be validated as strictly as possible on arrival, given the kind of content which it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
2. User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (&lt; &gt; &quot; &apos; etc).

Finding 9: Cleartext Password

Recommendations for Finding #9: Cleartext Password
1. Replace HTTP web services with HTTPs version in instances where data must be protected.
2. Replace unsecured services, such as telnet and rlogin, with a secured SSH service. If you must operate unsecured command line services, it is recommended that you operate them within a secured tunnel like SSL/TLS or VPN.
3. Training for user awareness.

Finding 10: Session Token in URL

Recommendations for Finding #10: Session Token in URL
1. The application should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.
Finding 11: SQL injection

Recommendations for Finding #11: SQL Injection

1. The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access.

Finding 12: Serialized Object in HTTP message

Recommendations for Finding #12: Serialized Object in HTTP Message

1. The best way to avoid vulnerabilities that arise from the use of serialized objects is not to pass these in request parameters, or expose them in any other way to the client.

Response for Findings 8, 9, 10, 11, and 12: NDUS CTS and campuses have already remediated, or are currently working to remediate, web application vulnerabilities identified in this assessment. NDUS CTS and campuses will need to develop an ongoing strategy to establish capabilities for identifying and remediating web application vulnerabilities. In addition, NDUS CTS and campuses will explore development platforms, secure coding standards, and training to facilitate secure application development. NDUS CTS and campuses will also explore exploit prevention technologies such as Web Application Firewalls (WAFs).
1. **Issue:** Election of the president of the State Board of Higher Education.

2. **Proposed motion:** Motion to elect ________ as the president of the State Board of Higher Education through June 30, 2015.

3. **Background:** Dr. Kirsten Diederich, president of the State Board of Higher Education, resigned on January 14, 2015. In accordance with SBHE Policy 310.2(2), Dr. Terry Hjemstad became the temporary president. The policy also requires the Board, at the next regular meeting of the Board, to elect a president to serve the balance of the unexpired term.

4. **Financial implications:** None.

5. **Academic implications:** None

6. **Legal/policy issues:** SBHE Policy 310.2(2) provides, in part: “In the event the office of the president becomes vacant during the elected term, the vice president shall act as temporary president until a new president is elected to fill the vacancy and serve the balance of the unexpired term.” SBHE Policy 310.2(4) also provides: “In the event an office is vacated, an election to fill the unexpired term shall be held at the next regular meeting of the Board.”

If the Board elects the current vice president to be president, the election will create a vacancy in the vice president position. Policy 310.2 provides that there should be “an election to fill the unexpired term…at the next regular meeting of the Board,” which would have the unintended result of leaving the position vacant for a month. However, it appears that the intent of the policy is to fill vacant officer positions as soon as possible, so the Board could elect a vice president to fill the unexpired term (through June 30, 2015, or until a successor is elected and qualified). The suggested motion would be: “Motion to elect ________ as the vice president of the State Board of Higher Education through June 30, 2015, or until a successor is elected and qualified.”

7. **Review Process:** N/A

8. **Enclosures:** None

9. **Key contact person(s) concerning issue:** Murray G. Sagsveen, Chief of Staff, Murray.Sagsveen@NDUS.edu, 701-328-1499.

10. **Chancellor’s Recommendation:** Recommend approval.
Summary of Proposed Action  
SBHE Meeting – January 29, 2015

1. **Issue:** Adoption of the Roles and Responsibilities Task Force Report

2. **Proposed motion:** Motion to approve the Roles and Responsibilities Task Force Report dated December 2014.

3. **Background:** The Roles and Responsibilities Task Force worked during 2013-2014 to review and update the 2006 task force on roles and responsibilities of NDUS leadership.

4. **Financial implications:** No significant implications.

5. **Academic implications:** The task force report addresses governance issues related to the SBHE, the chancellor, and the institution presidents, so will have indirect academic implications.

6. **Legal/policy issues:** Several policies address governance within the North Dakota University System, including:
   - [304.1](#) Chancellor/Commissioner of Higher Education: Authority and Responsibilities
   - [305.1](#) College and University Presidents' Authority and Responsibilities
   - [310.1](#) Board President and Member Responsibilities

   Also, statutes have been enacted to supplement the constitutional authority of the SBHE, such as [N.D.C.C. § 15-10-17](#).

7. **Review Process:**
   - Roles and Responsibilities Task Force
   - Chancellor’s Cabinet

8. **Enclosure:** Roles and Responsibilities Task Force Report

9. **Key contact person(s) concerning issue:** Dr. Larry Skogen, Interim Chancellor

10. **Chancellor’s Recommendation:** Recommend approval
1. **Issue:** Proposed modifications to *new tuition model*. The NDUS 2015-2020 Strategic Plan calls for implementation of new model by Fall 2017.

2. **Proposed motion:** Approve recommended new tuition model changes as follows: permit possible retention of separate distance ed fee for on-line courses; change in-country resident rate from 1.75 to 1.5 times the resident rate with the requirement that the rate change not be compensated for by a significant increase for the average full-time ND resident student.

3. **Background:** SBHE approved revised tuition model plan in June 2014. Upon further data analysis, the above changes are recommended to both minimize the financial impact to the institution and/or minimize the impact to students taking on-campus courses. Further, the reduction in the in-country rate from 1.75 to 1.5 (international students would remain at 1.75) would standardize the rate with WICHE and MHEC compact states and provide a positive recruiting tool. The NDUS Strategic plan calls for increasing enrollment of non-resident students.

4. **Financial implications:** Retention of the distance ed fee will help some campuses avoid a significant revenue loss, while also helping to avoid shifting all distance ed costs to on-campus students. It is estimated that most campuses (perhaps with the exception of 2 or 3) will retain a separate distance ed fee impacting about 6,400 distance ed students and generating about $4 million in revenue per year. Campuses estimate a slight revenue reduction as a result of the proposed in-country 1.75 to 1.5 rate change (estimated to be about $800,000-$1 M per year or less than 0.2% of total net tuition collections), most of the impact is at UND and NDSU. The lower rate will potentially generate more out-of-state enrollment which would allow the initial revenue reduction to be offset by new revenues from increased enrollments.

5. **Academic implications:** The proposed changes attempt to minimize financial impact to current students, especially on-campus students, while also trying to recruit additional non-resident students.

6. **Legal/policy issues:** Several 800 series SBHE policies will require updating once the details of the new model(s) are better defined. Further, legislative action to possibly limit or freeze tuition rates during the 15-17 biennium (e.g. 1043, 1233, 1303), would likely jeopardize our ability to implement a new tuition model, as under any new model, some students would pay less and some would pay more. If the new model had to be implemented under a tuition freeze, campuses would suffer a significant revenue loss.

7. **Review Process:** Admin. Affairs Council, Chancellor’s Cabinet, Glatt

8. **Enclosures:** “NDUS 2015-2020 Strategic Plan Tuition Model report to SBHE in June 2014, updated with recommended changes in January 2015

9. **Contact person:** Laura Glatt, VC For Administrative Affairs, 701-328-4116, laura.glatt@ndus.edu

10. **Chancellor’s Recommendation:** Approve
Summary of Proposed Action
SBHE Meeting – January 29, 2015

1. **Issue:** LRSC request to name the newly constructed technical education center.

2. **Proposed motion:** Motion to authorize LRSC to name the newly constructed technical education center, name to be announced at SBHE meeting January 29, 2015.

3. **Background:** In March 2013, the State Board of Higher Education ratified the Chancellor’s interim approval authorizing LRSC to access funds appropriated by the legislature ($5.6 million) to construct a new addition (24,000 square feet) to an existing technical education facility. No funds were appropriated to upgrade or renovate more than 30,000 square feet of classroom/laboratory resources in the aging buildings that would be enveloped by the new construction.

LRSC received “scope” approval to raise match-eligible funds to renovate the older, unfunded classroom/lab buildings and to provide state-of-the-art classroom technologies throughout the entire complex (new and old sections.) On August 20, 2014, the North Dakota Higher Education Challenge Fund Committee approved a match funding request for this project, contingent upon clarification that the proposed use of the funds did not exceed the project’s spending authorization. A memo from Laura Glatt clarified that using Challenge funds for FF&E was allowable because they were not part of the capital project.

While many donors participated in the effort to raise funds for classroom technologies and to renovate older classrooms, an individual family made a very significant gift, pledging $460,000 for the project. The North Dakota Higher Education Challenge Fund Committee approved matching funds for the family’s commitment in the amount of $230,000. For three generations, this community-minded family has played important roles in the college’s history and development. The current commitment and the multigenerational history of support for LRSC, make this gift especially significant.

LRSC wishes to recognize the generosity of this major donor family, To be announced at the January 29, 2015 Board meeting.

4. **Financial implications:** Minor expenses for anticipated signage.

5. **Academic implications:** This facility will be used for LRSC’s educational programs.

6. **Legal/policy issues:** The SBHE, in Policy 902.12, has reserved the final authority to name campus buildings, building additions, auditoriums and stadiums.

7. **Review Process:** Internal LRSC review and recommendation of President Darling
8. **Enclosures:** None.

9. **Key contact person concerning issue:** President Douglas Darling

10. **Chancellor’s Recommendation:** [The chancellor will add his recommendation.]
1. **Issue:** To permit University of North Dakota’s Police Department’s (UPD) to participate in joint law enforcement exercises in the state of Minnesota, an agreement must be signed by the president of the SBHE and witnessed by its secretary.

2. **Proposed motion:** Authorize UND’s request to enter into an agreement for the Joint Exercise of Peace Officer Duties. The purpose of this agreement is to grant the authority and set forth the conditions under which the participating criminal justice agencies may exchange or provide peace officers for the purpose of conducting or assisting in law enforcement and emergency response operations.

3. **Background:** This agreement codifies the original Grand Forks Narcotics Task Force agreement and extends its services into Minnesota. This agreement allows UPD to participate in and share resources with Minnesota when activities take officers across its border.

4. **Financial implications:** There are no financial implications to this agreement. If/when services are requested by an outside agency and costs are incurred, a fund is available to provide reimbursement to UPD for the incurred costs.

5. **Academic implications:** There are no academic implications to this agreement.

6. **Legal/policy issues:** This agreement for the Joint Exercise of Peace Officer Duties is made pursuant to NDCC § 54-40.3-04 and Minnesota Statute § 471.59.

7. **Review Process:** This agreement has been reviewed and signed by the East Grand Forks Chief of Police, East Grand Forks Mayor, and Pine to Prairie Drug Task Force Board Chair. Additionally, UND’s Vice President for Finance and Operations has reviewed this proposal.

8. **Enclosures:** Agreement for the Joint Exercise of Peace Officer Duties

9. **Contact person:** Eric Plummer, University of North Dakota Associate Vice President for Public Safety and Chief of Police, eric.plummer@und.edu, 701-777-3391

10. **Chancellor’s Recommendation:** [The chancellor will add his recommendation.]
1. **Issue:** The North Dakota University System (NDUS) maintains an inventory of accreditations of the academic programs of study offered by its eleven institutions. NDUS Procedure 420 requires that this inventory be updated in January and July each year.

2. **Proposed actions:** Accept the attached *Inventory* so it may be posted to the NDUS website.

3. **Background information:** The *North Dakota University System’s Academic Program Accreditation Inventory, Fall 2014,* lists all accreditations associated with specific academic programs of study. Additionally, all NDUS institutions are individually accredited by the Higher Learning Commission, a regional accrediting agency.

4. **Financial implications:** None

5. **Legal/policy issues:** The State Board of Higher Education (SBHE) Policy 420 - *Accreditation* states that “Institutions may apply, with the concurrence of the Chancellor, for accreditation of professional programs by agencies recognized by the U.S. Secretary of Education.” All such accreditations held by NDUS institutions are reported to the SBHE, as required by NDUS Policy 420 – *Accreditation Visits* on a bi-annual basis (July and January).

6. **Academic issues:** The *Inventory* summarizes any accreditation issues that may have been raised for a specific institution as a consequence of its most recent review by one or more accrediting agencies.

7. **Coordination:** The *Inventory* has been reviewed multiple times by individual institutions and twice by the Academic Affairs Council.

8. **Attachments:** *North Dakota University System’s Academic Program Accreditation Inventory, Fall 2014.*

9. **Contact information:** Sonia S. Cowen, Ph.D., Interim Vice Chancellor for Academic and Student Affairs, NDUS. Ph: 701-328-2965 / email: sonia.cowen@ndus.edu.

10. **Chancellor’s recommendation:** The Chancellor’s Cabinet approved this inventory at its meeting on 3 December 2014.

11. **SBHE Committee on Academic and Student Affairs recommendation:** The SBHE Committee on Academic and Student Affairs recommended at its meeting on 11 December 2014 that the SBHE accept this inventory.
1. **Issue:** WSC requires an additional $1.2M state general fund appropriation to complete the TrainND workforce training project in order to remediate soil conditions under the new parking lot.

2. **Proposed motion:** Authorize WSC to seek 15-17 state general fund appropriation of $1,200,000; and, increase spending for the Workforce Training project from $8,238,267 to $9,438,267 funded from $1,700,000 general fund, $2,500,000 financed through the Bank of North Dakota, $1,750,000 received as an oil impact grant from the Department of Trust Lands, $2,207,000 in private fundraising, $393,000 in approved state 13-15 Challenge funds, and $888,267 in local funds generated from training activities and to proceed with the project contingent upon receipt or guarantee of all funds.

3. **Background:** Engineers discovered artesian wells under the planned parking lot for this facility, which must be corrected at substantial cost prior to paving. There are no other viable funding sources for this work, and as a result WSC is seeking appropriations.

4. **Financial implications:** The cost of remediation increases the project cost by approximately 15%.

5. **Academic implications:** The parking lot is vital for the training mission of this facility as there are no other available parking areas that can be used by students.

6. **Legal/policy issues:** None

7. **Review Process:** Reviewed by Glatt, Tonder.

8. **Enclosures:** (agenda item and related material)

9. **Contact person:** President Nadolny (701.770.7475
raymond.nadolny@willistonstate.edu) & Deanette Piesik, CEO TrainND (701.774.4246
Deanette.piesik@willistonstate.edu)

10. **Chancellor’s Recommendation:** Approve
Summary of Proposed Action
SBHE Meeting – January 29, 2015

1. **Issue:** BSC requests authorization to refinance housing/auxiliary revenue bonds.

2. **Proposed motion:** 1) Authorize issuance of not-to-exceed $4,000,000 State Board of Higher Education of the State of North Dakota, BSC Housing and Auxiliary Facilities Revenue Refunding Bonds, Series 2015, for the purpose of refinancing the outstanding BSC Housing and Auxiliary Facilities Revenue Bonds, Series 2005, maturing on and after May 1, 2016, and paying the costs of issuance of the Series 2015; 2) Authorize the BSC President and/or Interim Executive Vice President to approve the sale of the bonds provided that the rate not exceed 4%, provided the present value of the debt service savings is not less than 2%. The approximate final date upon which the principal amount of the obligation will mature or become payable is May 2030; 3) Appoint the firm of Amstson Stewart Wegner PC as the bond counsel and Public Financial Management, Inc. as the financial advisor.

3. **Background:** The refinancing of the existing bonds requires SBHE approval as per NDCC 15-55.

4. **Financial implications:** Refinancing of the existing $3,335,000 outstanding bonds will take advantage of lower interest rates and subsequently reduce the overall carrying costs of the bonds. Financial advisors indicate the anticipated net present value savings will be approximately $476,000.

5. **Academic implications:** No significant implications

6. **Legal/policy issues:** No significant legal/policy issues.

7. **Review Process:** Reviewed by Glatt, external legal.

8. **Enclosures:** 1) SBHE request to issue and call; 2) BSC 2015 Board Resolution

9. **Contact person:** BSC Interim Executive Vice President Tamara Barber, tamara.barber@bismarckstate.edu (701) 224-5434

10. **Chancellor's Recommendation:** The Chancellor recommends his approval.
1. **Issue**: Authorize an inter-funding borrowing, and related planned fund deficit, of $500,000 for the purchase and installation of an electronic scoreboard for the MiSU Dome.

2. **Proposed motion**: Authorize MiSU to proceed with an inter-fund borrowing transaction of $500,000 to fund the purchase of an electronic scoreboard for the Dome.

3. **Background**: Funds to repay the inter-fund borrowing will be realized over a six-year period from long-term advertising partners. A similar interfund borrowing, and related fund deficit, approach was approved by the SBHE in May 2013 for the installation of an electronic scoreboard in the MiSU Herb Parker Stadium.

4. **Financial implications**: Interfunding borrowing eliminates financing and interest cost estimated to be a minimum of $70,000. This would require annual deficit disclosure to the SBHE and SAO until eliminated in FY2020.

5. **Academic implications**: None

6. **Legal/policy issues**: None

7. **Review Process**: Reviewed by Glatt

8. **Enclosures**: (agenda item and related material)

9. **Contact person**: Brian Foisy, MiSU VP for Administration and Finance, 701-858-3331 or at brian.foisy@minotstateu.edu

10. **Chancellor’s Recommendation**: Recommends approval.
1. **Issue**: Authorize a funding source change in the 15-17 budget request for the construction by Valley City Parks and Recreation of a Health, Wellness and Physical Education facility located on the VCSU campus to include student fees; and approve related student fee increase.

2. **Proposed motion**: Authorize funding source change for the construction by Valley City Parks and Recreation of a Health, Wellness and Physical Education Building, located on the VCSU campus from $15 million in private and $1 million in State Challenge Grant (up) to $13 million private, $1 million State Challenge Grant and $2 million student fee revenues; seek appropriate legislative authorization; and, further authorize an increase in the Fitness Facility fee from $0.42 per credit hour up to $12 per credit hour by no later than Fall 2017.

3. **Background**: 15-17 SBHE request originally did not include student fee revenues in support of this project; further, the SBHE has not yet approved the student fee increase.

4. **Financial implications**: The Fitness Facility Fee would increase from $0.42 per credit hour (up to 12 credit hours) or $10.00 per academic year to a per credit hour fee of $10-$12.00 per credit or $240-$288.00 per academic year. The final fee amount, not to exceed $12.00 per credit hour, will be determined once rates for other clientele are finalized. The fee, paid by approximately 1,380 full and part-time students, will generate about $250,000 in additional funds each year and will be remitted to VCPR. The increased student fee will be put in place reasonably close to when students have access to either existing or new wellness facility, but will occur no later than Fall 2017.

5. **Academic implications**: The facility is in response to significant growth in VCSU academic programs in Physical Education, Health, Exercise Science, and Athletic Training and the community desire and need for such a facility.

6. **Legal/policy issues**: Mandatory fee increase requires SBHE approval per NDCC 15-10.3-03, since it is over one percent (of tuition) increase; and further, campus-wide election since it is to support a construction project which exceeds $1 million. Campus-wide election occurred in October 2014, with 64% of voters in support of the fee increase.


8. **Enclosures**: (agenda item and related material)
9. **Contact person:** Doug Dawes, VCSU VP for Business Affairs, 701-845-7247 or doug.dawes@vcsu.edu

10. **Chancellor’s Recommendation:** Approve
Summary of Proposed Action
SBHE Meeting – January 29, 2015

1. **Issue:** UND College of Engineering and Mines plans to renovate three spaces within Upson II to provide for additional teaching and research labs, and collaborative space.

2. **Proposed motion:** Authorize UND to proceed with various classroom and laboratory upgrade projects for the College of Engineering and Mines (CEM) at an estimated cost of $1,375,000 to be funded from local funds.

3. **Background:** This project spans three areas:
   1) Upson II Hall Basement 1 – The proposed materials lab renovation brings together research, development and teaching capabilities that are currently scattered across several locations throughout CEM;
   2) Upson II Hall Basement 2 – The biomedical engineering lab will be used for undergraduate and graduate student teaching and research, and will provide students with a facility to enhance their problem solving skills and allow them to collaborate in teams; and
   3) Upson II east of south entrance – This project will expand the link that connects Upson I and II to create a space for students to gather, collaborate and study.

4. **Financial implications:** Funds for this project are derived from fees paid by the students enrolled in the distance education engineering program and the engineering program fee. All Distance students are required to conduct their labs on-campus during the summer. The renovated space will be utilized distance students as well. There are funds on hand to cover the project.

5. **Academic implications:** These projects support academic programs, and are required for teaching and research needs.

6. **Legal/policy issues:** There are no legal/policy issues related to this project.

7. **Review Process:** Tonder, Glatt

8. **Enclosures:** SBHE agenda item

9. **Contact person:** Alice Brekke, vice president for finance and operations, alice.brekke@und.edu, 701-777-3511

10. **Chancellor’s Recommendation:** Approve
1. **Issue:** DSU requests authorization to complete a deferred maintenance project at Pulver Hall at an estimated cost $566,195.

2. **Proposed motion:** Authorize DSU to proceed with replacement of the waste water risers in Pulver Hall at an estimated cost of $566,195 to be paid from local auxiliary funds.

3. **Background:** Recent failures to the waste water risers within Pulver Hall have prompted DSU to take action before additional failures and subsequent collateral damage may occur. Total cost of the project exceeds $250,000 and therefore requires SBHE authorization.

4. **Financial implications:** The project is funded by revenues generated by leasing the facility. Funding for the project is currently available.

5. **Academic implications:** None

6. **Legal/policy issues:** None

7. **Review Process:** Glatt, Tonder

8. **Enclosures:** Agenda item

9. **Contact person:** Mark Lowe, Vice President for Finance and Administration. 291 Campus Drive, Dickinson, ND 58601. PH (701) 483-2532 mark.lowe@dickinsonstate.edu

10. **Chancellor's Recommendation:** Approve.
1. Issue: NDSU intends to renovate Music Education building south entry constructed in 1982 to address deferred maintenance issues and provide ADA compliance.

2. Proposed motion: Authorize NDSU to proceed with the Music Building South Entry Renovation project at an estimated cost of $350,000 funded from appropriated operations funding.

3. Background: The Music Education building south entry has not been renovated since its' construction and does not meet current ADA requirements. The seals for the arched insulated glass panels and portions of the brick on the arched soffit/wall system have failed.

4. Financial implications: The project will be funded from FY14 appropriated capital project designated reserves per SBHE policy 810.1, which are sufficient and available for the project.

5. Academic implications: None

6. Legal/policy issues: None

7. Review Process: Glatt, Tonder

8. Enclosures: Agenda item

9. Contact person: Bruce Bollinger, VP Finance and Administration, Old Main 11E, PO Box 6050, Fargo, ND (701) 231-8412
   
   bruce.bollinger@ndsu.edu

10. Chancellor’s Recommendation: Approve
1. **Issue:** Proposed amendment to SBHE Policy 903 (Sale or Removal of Buildings).

2. **Proposed motion:** Motion to amend SBHE Policy 903 to include a new paragraph that would state:

   If the director of the State Historical Society determines that an institution-owned building may have historical significance, the president (or dean) of the institution shall inform the Chancellor of the institution’s plan to sell, remove, demolish, or alter the building. The Chancellor shall forward the plan to the SBHE with the Chancellor’s recommendation. Unless the SBHE acts on the plan within sixty days after the Chancellor is informed of the institution’s plan, the institution may implement the plan.

3. **Background:** Currently, the SBHE is not involved in the sale, removal, alteration, or demolition of a building that may have historical significance. The proposed amendment to Policy 903 would provide an opportunity for the SBHE to participate in the process if it chooses to do so.

4. **Financial implications:** The proposed policy amendment, if adopted, could lengthen the time involved to sell, remove, alter, or demolish a building.

5. **Academic implications:** Not applicable.

6. **Legal/policy issues:** The 55-02-07. Protection of historical or archaeological artifacts or sites. Any historical or archaeological artifact or site that is found or located upon any land owned by the state or its political subdivisions or otherwise comes into its custody or possession and which is, in the opinion of the director of the state historical society, significant in understanding and interpreting the history and prehistory of the state, may not be destroyed, defaced, altered, removed, or otherwise disposed of in any manner without the approval of the state historical board, unless section 55-02-07.2 applies to the site. Notification of the director's opinion of significance must be communicated to the appropriate governing official. The state historical board through the director, within sixty days of written notification to it by the appropriate governing official of the state or political subdivision's desire, need, or intent to destroy, alter, remove, or otherwise dispose of a significant artifact or site, shall provide the governing official written direction for the care, protection, excavation, storage, destruction, or other disposition of the significant artifact or site. The state and its political subdivisions shall cooperate with the director in identifying and implementing any reasonable alternative to destruction or alteration of any historical or archaeological artifact.
or site significant in understanding and interpreting the history and prehistory of the state before the state historical board may approve the demolition or alteration.

7. Review Process:
   • Vice Chancellor Laura Glatt
   • Rick Tonder, Director of Facilities Planning

8. Enclosures: Policy 903 showing proposed amendments.

9. Key contact person(s) concerning issue: Grant Shaft, member, SBHE

10. Chancellor’s Recommendation: