WWAMI

Idaho WWAMI
(Washington, Wyoming, Alaska, Montana, Idaho) Medical Education Program

Strategic Plan
FY2018-FY2022

WWAMI is Idaho's medical school, and is under the leadership and institutional mission of the University of Idaho, in partnership with the University of Washington School of Medicine (UWSOM). In August 2015, we began the new 2015 WWAMI medical school curriculum at all six regional WWAMI sites. Students started with a multi-week clinical immersion experience—intensively learning the clinical skills and professional habits to serve them throughout their careers. For their first 18 months, students spend a full day each week learning and practicing clinical skills in a community primary care clinic and in workshops. This is in addition to their hospital-based "Colleges" training with a faculty mentor and small group of peers. This new curriculum allows our students to be on the University of Idaho campus for up to 4 terms, instead of the previous 2 terms. It also provides our medical students with the option to spend the majority of all four years of medical education in the State of Idaho. Over the past four years, the Idaho State Legislature appropriated funding to continue the support for 5 more first-year medical students in the Idaho WWAMI Targeted Rural and Underserved Track program (TRUST). The mission of TRUST is to provide a continuous connection between underserved communities, medical education, and health professionals in our region. This creates a full-circle pipeline that guides qualified students through a special curriculum connecting them with underserved communities in Idaho. In addition, this creates linkages to the UWSOM's network of affiliated residency programs. The goal of this effort is to increase the medical workforce in underserved regions. In addition, the State of Idaho appropriated funding for 5 additional traditional WWAMI students, expanding the Idaho class size to 40 medical students starting in fall 2016.

As the medical education contract program for the State of Idaho with the University of Washington, the UI-WWAMI Medical Program supports the Strategic Action Plan of its host university, the University of Idaho, while recognizing its obligation to the mission, goals, and objectives of its nationally accredited partner program, the UWSOM.

MISSION STATEMENT

The University of Washington School of Medicine is dedicated to improving the general health and well-being of the public. In pursuit of its goals, the School is committed to excellence in biomedical education, research, and health care. The School is also dedicated to ethical conduct in all of its activities. As the preeminent academic medical center in our region and as a national leader in biomedical research, we place special emphasis on educating and training physicians, scientists, and allied health professionals dedicated to two distinct goals:

- Meeting the health care needs of our region, especially by recognizing the importance of primary care and providing service to underserved populations.
- Advancing knowledge and assuming leadership in the biomedical sciences and in academic medicine.

The School works with public and private agencies to improve health care and advance knowledge in medicine and related fields of inquiry. It acknowledges a special responsibility to the people in the states of Washington, Wyoming, Alaska, Montana, and Idaho, who have joined with it in a unique regional partnership. The School is committed to building and sustaining a diverse academic community of faculty, staff, fellows, residents, and students and to assuring that access to education and training is open to learners from all segments of society, acknowledging a particular responsibility to the diverse populations within our region.

The School values diversity and inclusion and is committed to building and sustaining an academic community in which teachers, researchers, and learners achieve the knowledge, skills, and attitudes that value and embrace inclusiveness, equity, and awareness as a way to unleash creativity and innovation.

VISION STATEMENT

Our students will be highly competent, knowledgeable, caring, culturally sensitive, ethical, dedicated to service, and engaged in lifelong learning.

GOAL 1

A WELL EDUCATED CITIZENRY – Continuously improve access to medical education for individuals of all backgrounds, ages, abilities, and economic means.

Objective A:

Access - Provide outreach activities that help recruit a strong medical student applicant pool for Idaho WWAMI.

Performance Measures:
The number of Idaho WWAMI medical school applicants per year and the ratio of Idaho applicants per funded medical student seat.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
(158) 7.9:1	**(157) 6.28:1**	**(141) 4.7:1**	**(164) 4.7:1**	**5:1**

Benchmark: National ratio of state applicants to medical school per state-supported seats.[1]
The benchmark is the national ratio of state applicants to medical school to the number of state supported positions. The ratio of applicants in Idaho to the number of available positions was 4.7:1; the national ratio of in-state applicants to available positions is 16:1.
https://www.aamc.org/download/321442/data/factstablea1.pdf

Objective B:

Transition to Workforce - Maintain a high rate of return for Idaho WWAMI graduate physicians who choose to practice medicine in Idaho, equal to or better than the national state return rate.

Performance Measure:
Cumulative Idaho WWAMI return rate for graduates who practice medicine in Idaho.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
51%	**50%**	**51%**	**51%**	**41%**

Benchmark: target rate – national average or better.[2] *The benchmark is 41%, the national average of students that return to their native state to practice medicine. In Idaho, the return rate was 51% (296/586).*

GOAL 2

CRITICAL THINKING AND INNOVATION - WWAMI will provide an environment for the development of new ideas, and practical and theoretical knowledge to foster the development of biomedical researchers, medical students, and future physicians who contribute to the health and wellbeing of Idaho's people and communities.

Objective A:
Critical Thinking, Innovation and Creativity – Generate research and development of new ideas into solutions that benefit health and society.

Performance Measure:
WWAMI faculty funding from competitive federally funded grants**.**

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
$1.4M	**$2.3M**	**$4.4M**	**$1M**	**$1.4M**

Benchmark: $1.4M [3] The benchmark for this objective is $1.4M annually, through FY 2022. In FY17, WWAMI-affiliated faculty at UI successfully brought in $1M of research funding into Idaho from agencies such as the National Institute of Health (NIH) and the Department of Health and Human Services (DHHS). In addition, WWAMI has had a long standing relationship with the Idaho INBRE Program, where each year our medical students apply for summer research fellowships. INBRE received a $16.3 million renewal grant from NIH in 2013.

Objective B:
Innovation and Creativity – Educate medical students who will contribute creative and innovative ideas to enhance health and society.

Performance Measures:
Percentage of Idaho WWAMI medical students participating in medical research (laboratory and/or community health).

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
100%	**100%**	**100%**	**100%**	**100%**

Benchmark: Internally set benchmark as measure of program quality - 100% [4] The benchmark is 100% of Idaho WWAMI students participating in medical research. All students at the UWSOM must participate in a research activity.

Objective C:
Quality Instruction – Provide excellent medical education in biomedical sciences and clinical skills.

Performance Measure:
Pass rate on the U.S. Medical Licensing Examination (USMLE), Steps 1 & 2, taken during medical training.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
100%	**100%**	**100%**	**100%**	**91%**

Benchmark: U.S. medical student pass rates, Steps 1 & 2 [5] The benchmark for the U.S. Medical Licensing Examination (USMLE), Steps 1 & 2, is the U. S. medical student pass rates.

GOAL 3
EFFECTIVE AND EFFICIENT DELIVERY SYSTEMS – Deliver medical education, training, research, and service in a manner which makes efficient use of resources and contributes to the successful completion of our medical education program goals for Idaho.

Objective A:
Increase medical student early interest in rural and primary care practice in Idaho.

Performance Measure:
The number of WWAMI rural summer training placements in Idaho each year.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
21	**26**	**23**	**22**	**20**

Benchmark: 20 rural training placements following first year of medical education [6] *The benchmark is 20 rural training placements following the first year of medical education. During the past summer, 22 students completed a Rural Underserved Opportunities Program (RUOP) experience in Idaho.*

Objective B:
Increase medical student participation in Idaho clinical rotations (clerkships) as a part of their medical education.

Performance Measure:
The number of WWAMI medical students completing at least one clerkship in Idaho each year.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
30	**34**	**36**	**24**	**20**

Benchmark: 20 clerkship students each year [7] *The benchmark is 20 clerkship students per year that complete at least one clerkship in Idaho. The Idaho Track is a voluntary program of the University of Washington School of Medicine in which students complete the majority of required clinical clerkships within Idaho. Third-year Idaho Track medical students complete approximately twenty-four weeks of required clerkships in Idaho, and fourth-year Idaho Track medical students complete three of four required clerkships in Idaho. Twelve third-year students and twelve fourth-year students participated in the Idaho Track during the 2015-2016 academic year. In addition to Idaho Track students, other UWSOM students rotated among the various clinical clerkships in Idaho. During academic year 2015-16, a total of 105 UWSOM students completed one or more clinical rotations in Idaho. Those 105 medical students completed a total of 231 individual clinical rotations in Idaho.*

Objective C:
Support and maintain interest in primary care and identified physician workforce specialty needs for medical career choices among Idaho WWAMI students.

Performance Measure:
Percent of Idaho WWAMI graduates choosing primary care, psychiatry, general surgery, and OB/GYN specialties for residency training each year.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
65%	**64%**	**47%**	**59%**	**50%**

Benchmark: 50% or more of Idaho WWAMI graduating class choosing needed work force specialties for residency training each year [8] *The benchmark is 50% of the Idaho WWAMI graduating class choosing a specialty for residency training that is needed in the state (primary care, psychiatry, general surgery, and OB/GYN specialties).*

Objective D:
Maintain a high level Return on Investment (ROI) for all WWAMI graduates who return to practice medicine in Idaho.

Performance Measure:
Ratio of all WWAMI graduates who return to practice medicine in Idaho, regardless of WWAMI origin, divided by the total number of Idaho medical student graduates funded by the State.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
75%	**72%**	**75%**	**75%**	**60%**

Benchmark: target ratio – 60% [9] *The benchmark for the Return on Investment (ROI) for all WWAMI graduates who return to practice medicine in Idaho is 60%. The current ROI is 75% (440/586).*

Objective E:
Efficiently deliver medical education under the WWAMI contract, making use of Idaho academic and training resources.

Performance Measure:
Percent of Idaho WWAMI medical education contract dollars spent in Idaho each year.

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
67%	**72%**	**70%**	**70%**	**50%**

Benchmark: 50% [10] *The benchmark for this objective is 50%, the percentage of Idaho WWAMI medical education dollars spent in Idaho each year. In FY17, 70% of the State appropriations were spent in Idaho.*

Key External Factors *(beyond the control of the Idaho WWAMI Medical Program)*:

Funding: the number of state-supported Idaho medical student seats each year is tied to State legislative appropriations. Availability of revenues and competing funding priorities may vary each year.

Medical Education Partnerships: as a distributed medical education model, the University of Idaho and the UWSOM WWAMI Medical Program rely on medical education partnership with local and regional physicians, clinics, hospitals, and other educational institutions in the delivery of medical training in Idaho. The availability of these groups to participate in a distributed model of medical education varies according to their own budget resources and competing demands on their time and staff each year.

Population Changes in Idaho: with a growing population and an aging physician workforce, the need for doctors and medical education for Idaho's students only increases. Changes in population statistics in Idaho may affect applicant numbers to medical school, clinical care demands in local communities and hospitals, and availability of training physicians from year to year.

New Medical School Curriculum: The University of Washington School of Medicine engaged in a major review and revision of the medical school curriculum which has impacted delivery of education and training in the WWAMI programs in Idaho. Given that students are on the University of Idaho campus for up to four terms instead of two, adjustments must be made to accommodate the increased number of medical students on campus. Expanded facilities, enhanced technology, additional faculty and support staff are necessary for the additional students and delivering this new state of the art curriculum. The University of Idaho is already anticipating these needs and working toward expanding facilities to accommodate the increased number of students. Tuition funds from third term medical students will help support the program's needs. The University of Idaho has identified and hired the necessary faculty to support the programmatic changes implemented in fall 2015. This curriculum renewal offers Idaho the opportunity to keep Idaho students in-state all four years of their medical education, which is a significant advantage in retaining students as they transition to clinical practice.

For-profit Medical Schools in Idaho: There is an increasing need for more high quality clerkships for our students. The current challenge in developing clinical training opportunities is that multiple health profession training programs, such as medical students, physician assistant students, nurse practitioner students, family medicine residents, internal medicine residents and psychiatry residents are all seeking clinical training sites in Idaho. The proposed introduction of a for-profit medical school in Idaho adding up to 300 additional clerkship students needing clinical training, would create significant challenges for clinicians in Idaho to meet those needs. The saturation of clinical training sites in Idaho has the potential to impact clinical opportunities for Idaho's only public supported medical education program housed in Idaho (WWAMI). Without strategic and thoughtful growth for medical education, the states only allopathic medical education opportunities for Idaho residents may be negatively impacted.

Evaluation Process

The metrics will be reviewed annually to evaluate their continued appropriateness in assessing the various goals and processes. As the feedback from the annual review process is reviewed the effectiveness of the processes will be refined. These feedback cycles are in place for Strategic Plan Metrics, Program Prioritization Metrics, External Program Review Process as well as a continued examination of various elements of community need as well.

Cyber Security Plan

The WWAMI Medical Education Program has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework and implementation of the Center for Internet Security (CIS) Controls through the University of Idaho, which follows the Executive Order from the State Board of Idaho, https://gov.idaho.gov/mediacenter/execorders/eo17/EO%202017-02.pdf

[1] Based on nationally set standards. The benchmark is the national ratio of state applicants to medical school to the number of state supported seats.

[2] Based on national set standards. 41% is the national average of students that return to their native state to practice medicine

[3] Based on available resources for pursuing external grants and increased competitive nature of federal awards.

[4] Internally set benchmark as measure of program quality. All students at the UWSOM must participate in a research activity.

[5] Based on national standards

[6] Based on state needs and available resources

[7] Based on analysis of areas of increase need in Idaho

[8] Based on national standards for workforce specialties

[9] Based on national standards for program return rates

[10] Based on available Idaho resources

Appendix 1

	State Board of Education Goals			
	Goal 1: A WELL EDUCATED CITIZENRY	*Goal 2: INNOVATION AND ECONOMIC DEVELOPMENT*	*Goal 3: DATA-INFORMED DECISION MAKING*	*Goal 4: EFFECTIVE AND EFFICIENT EDUCATIONAL*
Institution/Agency Goals and Objectives				
GOAL 1: A WELL EDUCATED CITIZENRY ***Continuously improve access to medical education for individuals of all backgrounds, ages, abilities, and economic means.***	✓	✓	✓	
Objective A: Access - Provide outreach activities that help recruit a strong medical student applicant pool for Idaho WWAMI.	✓		✓	✓
Objective B: Transition to Workforce - Maintain a high rate of return for Idaho WWAMI graduate physicians who choose to practice medicine in Idaho, equal to or better than the national state return rate.	✓			✓
GOAL 2: CRITICAL THINKING AND INNOVATION WWAMI will provide an environment for the development of new ideas, and practical and theoretical knowledge to foster the development of biomedical researchers, medical students, and future physicians who contribute to the health and wellbeing of Idaho's people and communities.	✓	✓		
Objective A: **Critical Thinking, Innovation and Creativity – Generate research and development of new ideas into solutions that benefit health and society.**	✓	✓		✓
Objective B: Innovation and Creativity **- Educate medical students who will contribute creative and innovative ideas to enhance health and society.**	✓	✓		
Objective C: Quality Instruction – Provide excellent medical education in biomedical sciences and clinical skills.	✓			✓
GOAL 3: EFFECTIVE AND EFFICIENT DELIVERY SYSTEMS Deliver medical education, training, research, and service in a manner which makes efficient use of resources and contributes to the successful completion of our medical education program goals for Idaho.	✓		✓	✓

Objective A: Increase medical student early interest in rural and primary care practice in Idaho.		✓		✓
Objective B: Increase medical student participation in Idaho clinical rotations (clerkships) as a part of their medical education.				
Objective C: Support and maintain interest in primary care and identified physician workforce specialty needs for medical career choices among Idaho WWAMI students.				✓
Objective D: Maintain a high level Return on Investment (ROI) for all WWAMI graduates who return to practice medicine in Idaho.		✓		✓
Objective E: Efficiently deliver medical education under the WWAMI contract, making use of Idaho academic and training resources.	✓	✓		✓

Cybersecurity Overview and Critical Security Controls Assessment Report

Date: June 19, 2017

Status: FINAL

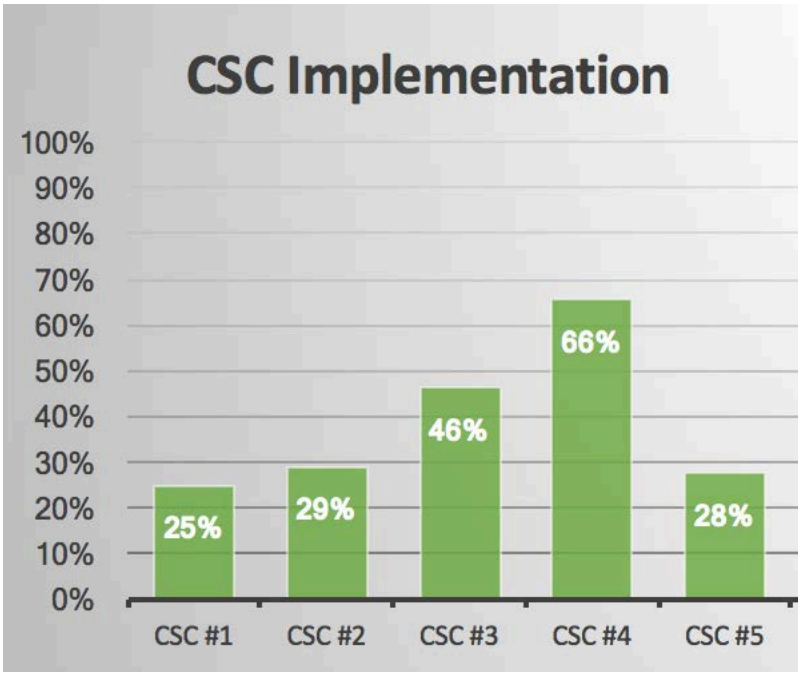
Author: Mitch Parks mitch@uidaho.edu

Contents

Executive Summary

In response to increasing cybersecurity threats and the Idaho Governor's Executive Order 2017-02 issued January 16, 2017, UI ITS personnel initiated an assessment of current cybersecurity measures as well as UI's status in respect to the Center for Internet Security (CIS) Critical Security Controls (CSC) 1-5. The CSC assessment was scored using the AuditScripts initial assessment tool recommended by the State Office of the CIO and acting Chief Information Security Officer, Lance Wyatt. Direction from the State Office of the CIO was to complete only the assessment by June of 2017, with any new implementation activities to occur in Fiscal Year 2018.

Between March 2 and May 15, 2017, the ITS team reviewed each of the Critical Security Controls from version 6.1 of CIS. That assessment shows a 0.39 (out of 1.0) overall implementation for the first 5 controls.



Overall completion for each control combines scoring for policy, implementation, automation and reporting. A 100% score could be achieved by approving the written policy, implementing and automating a control for all systems, and reporting it to the executive level. For some specific controls, 100% implementation will not be desirable or achievable on a university network. Prioritization, scope, and target percentage of specific controls will be assessed and prioritized.

The results of this assessment will be used within the FY18 IT Security Plan and will be prioritized with other technology risks to meet the goals of our target profile under the NIST Cybersecurity Framework.

High Level Cybersecurity Assessment

Summarized below are several measures taken by the University to protect its technology and information from internal and external breaches.

Policies/Procedures

The University has established policies and procedures over the following areas:

- Administrative Systems and Applications
- Information Technology Services (ITS) Security Access
- User Provided Software on ITS Systems
- Computer User Account Procedures
- University Data Classification and Standards
- Acceptable Use of Technology Resources
- Networked Computing Device Standards
- Proactive UI Network Security Measures
- UI Password/Pass-phrase Policy
- Managing Systems for Employee Turnover
- Computer File Backup and Recovery
- Scheduling and Notification of Central Computer System Outages
- Computer Security Violations
- Banner Training and Authorization
- Payment Card Processing

External Review

In 2013, the University engaged an external higher education consulting team to provide an objective view of the state of information technology policy and security at the University. Many recommendations were implemented, including the establishment of an Information Security Office, the hiring of an Information Security Officer, and the development of a number of policies, standards, and best practices.

Technology Security Advisory Council

In 2014, the University formed a nine-member council to advocate for improved security, identify potential IT security issues, and advise the Information Security Officer on strategies, priorities, and communication. This council meets monthly.

Employee Training and Awareness

In 2017, the University required all employees to complete an on-line training module on cyber security risk. The University has achieved a 96% completion rate. In addition, the University Information Security Officer has conducting phishing awareness campaigns to educate employees on how to protect their data and devices from phishing attacks.

Encryption

The University has implemented the first phase of a device encryption program based on the University data classification policy. This project has encrypted 338 devices as of June 19, 2017, representing 95% of identified devices with potentially high risk data.

Governor's Executive Order No. 2017-02

Two of the ten directives listed in the EO are:

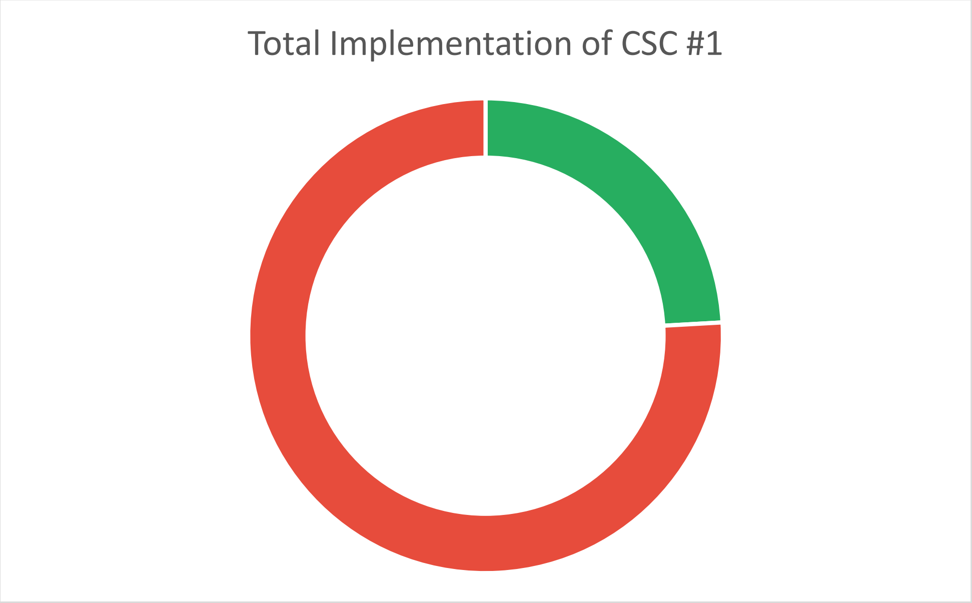
- Adoption and implementation of the National Institute of Standards and Technology (NIST) cybersecurity framework; and
- Implementation of the first five Center for Internet Security (CIS) critical security controls.

The University has adopted the NIST framework and has conducted a self-assessment of the CIS controls (no.'s 1-5) and is discussed later in this document. The results of the self-assessment have been communicated to the University President. The University Information Security Officer is also near completion of a cyber security strategic plan which will outline recommended action items for the University going forward.

Critical Security Controls

Using the AuditScripts tool, the following pages show the overall risk for each control. This assumes that any control not fully implemented has been implicitly, if not explicitly, accepted as a risk. Detailed answers on each control are not provided, but are on file in the ITS Information Security Office.

CSC #1: Inventory of Authorized and Unauthorized Devices

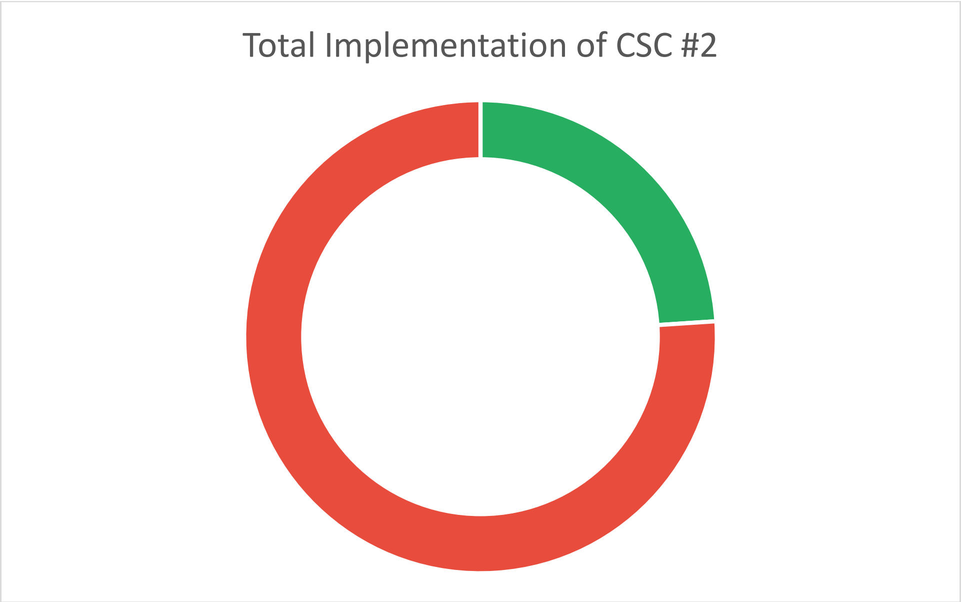

Total Implementation of CSC #1

Risk Addressed:	24%
Risk Accepted:	76%

ID	Critical Security Control Detail
1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization’s public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.
1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.

CSC #2: Inventory of Authorized and Unauthorized Software

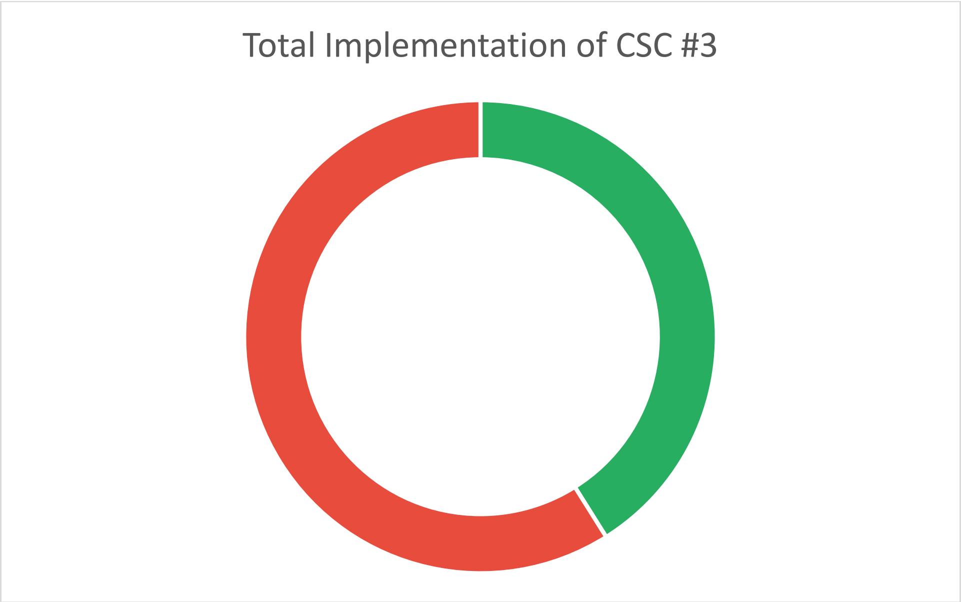

Total Implementation of CSC #2

Risk Addressed:	24%
Risk Accepted:	76%

ID	Critical Security Control Detail
2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
2.2	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and Protects execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

CSC #3: Secure Configurations for Hardware and Software



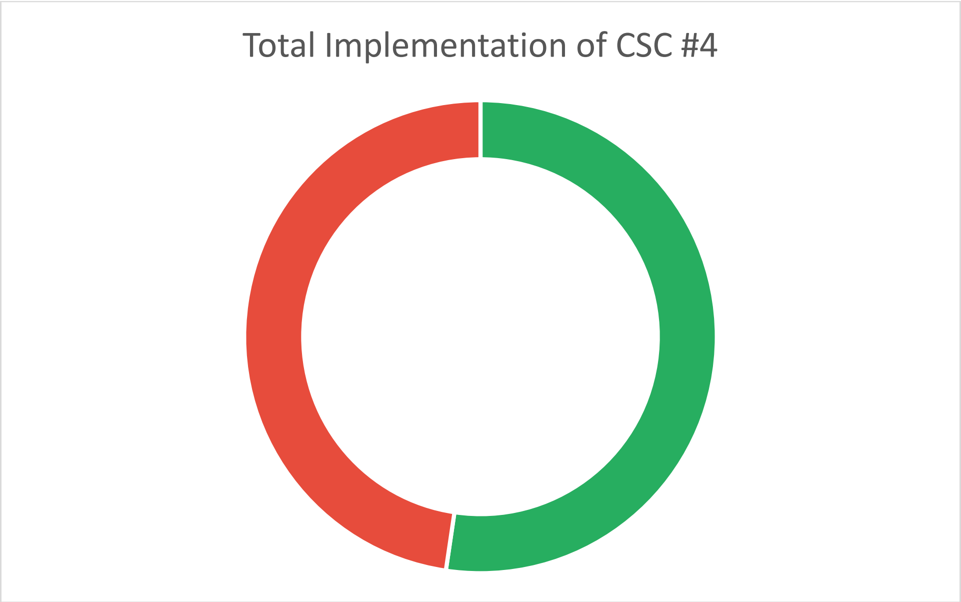
Risk Addressed:	**41%**
Risk Accepted:	**59%**

ID	Critical Security Control Detail
3.1	Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be

	created for workstations, servers, and other system types used by the organization.
3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.
3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.
3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).
3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.

3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.

CSC #4: Continuous Vulnerability Assessment and Remediation

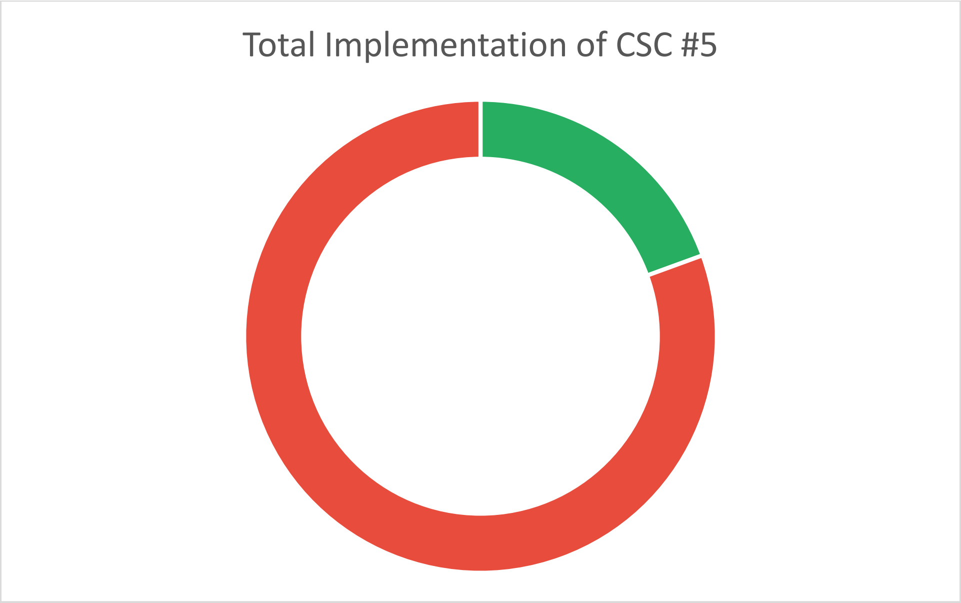


Risk Addressed:	52%
Risk Accepted:	48%

ID	Critical Security Control Detail
4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

4.2	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.
4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.
4.4	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.
4.5	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.
4.6	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.
4.7	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.
4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.

CSC #5: Controlled Use of Administrative Privileges


Total Implementation of CSC #5

Risk Addressed:	19%
Risk Accepted:	81%

ID	Critical Security Control Detail
5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.

5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.
5.6	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.
5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.
5.9	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Appendix A: References

Tracking of key references useful for this report.

Executive Order 2017-01	Findings of the Idaho Cybersecurity Taskforce	https://gov.idaho.gov/mediacenter/execorders/eo17/EO%202017-02.pdf
Critical Security Controls	Version 6.1	https://www.cisecurity.org/controls/
Audit Scripts	Free Assessment Resources	http://www.auditscripts.com/free-resources/critical-security-controls/