



University of Idaho

AGRICULTURAL RESEARCH & EXTENSION SERVICE

STRATEGIC PLAN FY2018-FY2022

MISSION STATEMENT

The University of Idaho, College of Agricultural and Life Sciences fulfills the intent and purpose of the only land-grant University in the state that serves the agricultural/food-industry, people and communities of Idaho and our nation:

- Through identification of critical needs and development of creative solutions,
- Through the discovery, application, and dissemination of science-based knowledge,
- By preparing individuals through agricultural, food and family consumer education and research to become leaders and contributing members of society

VISION STATEMENT

Through focused areas of excellence in teaching, research and outreach with Extension serving as a critical knowledge bridge between the University of Idaho, College of Agricultural and Life Sciences, and the people of Idaho, we will be the recognized as the state-wide leader and innovator in meeting current and future challenges to support healthy individuals, families and communities, and enhance sustainable food systems.

GOAL 1

Innovate: Scholarly and creative products of the highest quality and scope, resulting in significant positive impact for the region and the world.

Objective A: Build collaborations that increase scholarly and creative productivity through interdisciplinary, regional, national and global partnerships.

Performance Measures:

- I. Increases in sponsored research expenditures and scholarly/creative works derived from collaborative Federal and Corporate partnerships.

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
\$15,647,292	\$16,535,798	\$16,843,795	\$28,770,264	\$34,353,200

Benchmark: \$34,353,200 in research expenditures grant dollars by 2023. ¹

- II. Increase of undergraduate and graduate students engaged and employed on sponsored projects

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
12%	12.36%	13.60%	14.00%	16.72%

Benchmark: 16.72% of our undergraduate and graduate students will be paid from sponsored projects by 2023. ²

- III. Increase the number of Advanced/Graduate degrees in the area of Agricultural and Life Sciences

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
-	45	46.80	49.14	53.73

Benchmark: 53.73 Advanced/Graduate degrees will be awarded in the area of Agricultural and Life Sciences by 2023. ³

GOAL 2

Engage: Outreach that inspires innovation and culture

Objective A: Increase the number of individuals/families benefiting from U of I Outreach Extension Programs

Performance Measures:

- I. Increase the number of direct educational and programmatic University of Idaho Extension Contacts

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
375,350	358,662	338,261	348,409	403,901

Benchmark: 403,901 Direct Contacts will be made from the U of I Extension Programs by 2023. ⁴

Objective B: Increase the number of youth participating in University of Idaho 4-H Youth Development programming

Performance Measures:

- I. Increase the number of youth participating in U of I 4-H Youth Development Programming

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
56,546	55,742	54,786	56,430	67,380

Benchmark: 67,380 youth participating in the U of I Youth Development Programming by 2023. ⁵

Objective C: Increase the number of publications from University of Idaho Extension

Performance Measures:

I. Increase Peer Reviewed and Professional Scientific Publications from University of Idaho Extension

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
-	-	88	91	102

Benchmark: 102 University of Idaho Extension Peer Reviewed and Professional Scientific Publications will be published by 2023. ⁶

Objective D: Increase the educational and research web traffic accessed from the University of Idaho Extension network

Performance Measures:

I. Increase educational and research web traffic and views of U of I Extension Content

FY14 (2013-2014)	FY15 (2014-2015)	FY16 (2015-2016)	FY17 (2016-2017)	Benchmark
-	-	499,574	514,561	562,275

Benchmark: 562,275 web visits will be trafficked to the University of Idaho Extension websites by 2023 ⁷

Key External Factors

- Changes in county, state, federal and industry supported research and extension funding could impact ARES activities.
- Change in the public's trust in research based education.
- Maintenance and replacement of ageing infrastructure continues to impact research and extension productivity. Finding resources to meet these needs is imperative.
- Comparison of salary and benefits with peer institutions continues to hamper our ability to hire and retain highly qualified individuals within the Agricultural Research and Extension Service.

Evaluation Process

In conjunction with the Federal Agricultural Research and Extension Services (ARES) funding, the evaluation process for this strategic plan is documented through the Plan of Work identified by the USDA and a peer review panel of best practices in research and extension across all land grant institutions. The measurements used are of those that correlate with the National and State Agenda for the agricultural, family consumerism, research and education of our citizenry.

¹ Based on review of available resources.

² Based on review of available and expected resources.

³ Based on review of current students in the program and expected capacity limits.

⁴ Based on review of available and projected resources.

⁵ Based on review of program capacity and current participation trends.

⁶ Based on review of historical trends.

⁷ Based on review of historical trends and site improvement impacts.

Cybersecurity Overview and Critical Security Controls Assessment Report



Date: June 19, 2017

Status: FINAL

Author: Mitch Parks mitch@uidaho.edu

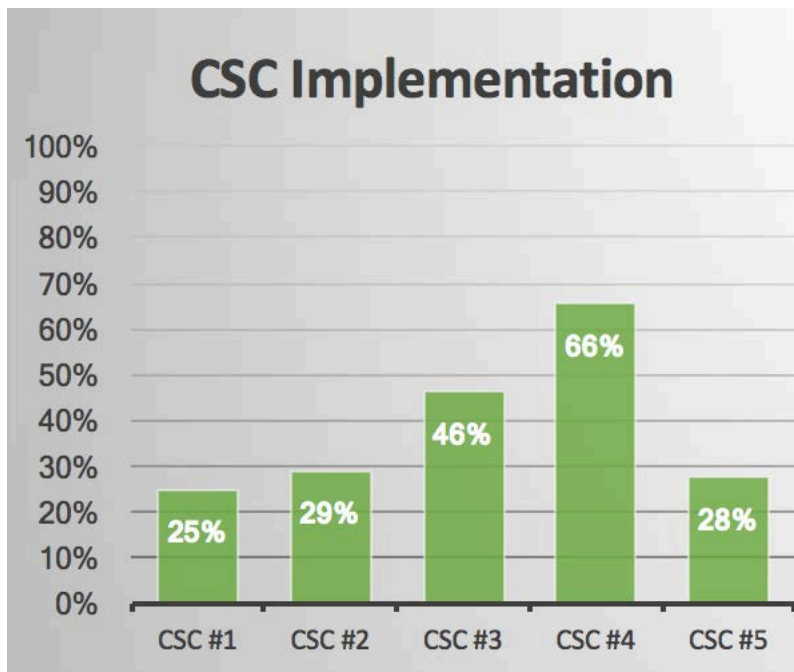
Contents

Cybersecurity Overview and Critical Security Controls Assessment Report.....	1
Executive Summary.....	3
High Level Cybersecurity Assessment.....	4
Critical Security Controls.....	6
CSC #1: Inventory of Authorized and Unauthorized Devices.....	6
CSC #2: Inventory of Authorized and Unauthorized Software	8
CSC #3: Secure Configurations for Hardware and Software.....	10
CSC #4: Continuous Vulnerability Assessment and Remediation.....	13
CSC #5: Controlled Use of Administrative Privileges	15
Appendix A: References.....	17

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:

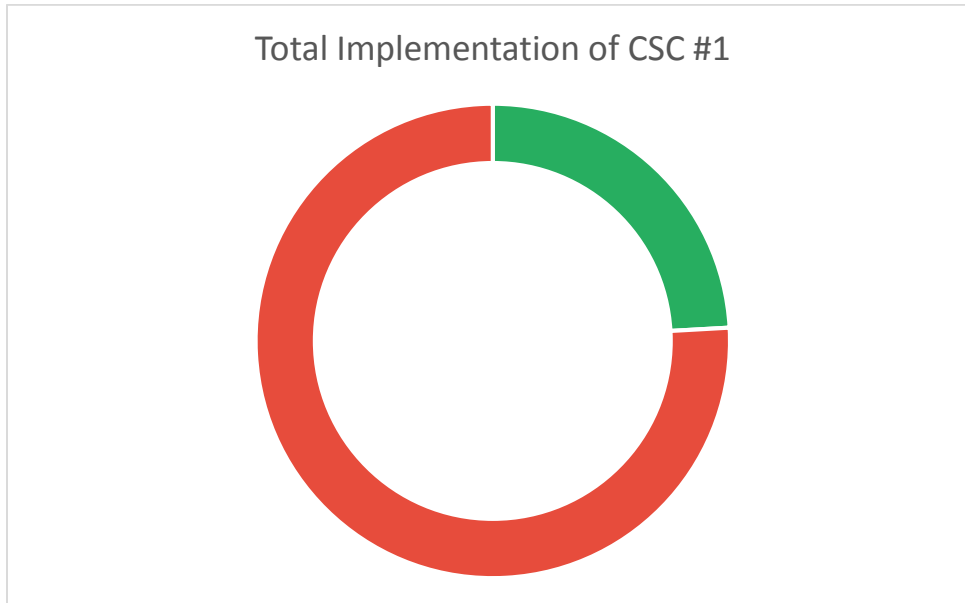
- Adoption and implementation of the National Institute of Standards and Technology (NIST) cybersecurity framework; and
- Implementation of the first five Center for Internet Security (CIS) critical security controls.

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



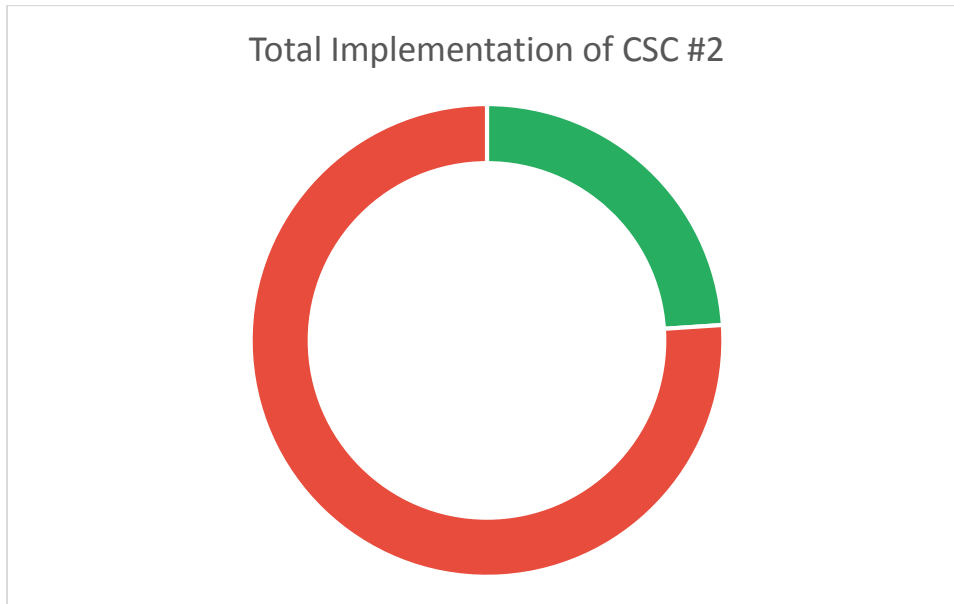
Risk Addressed: 24%

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



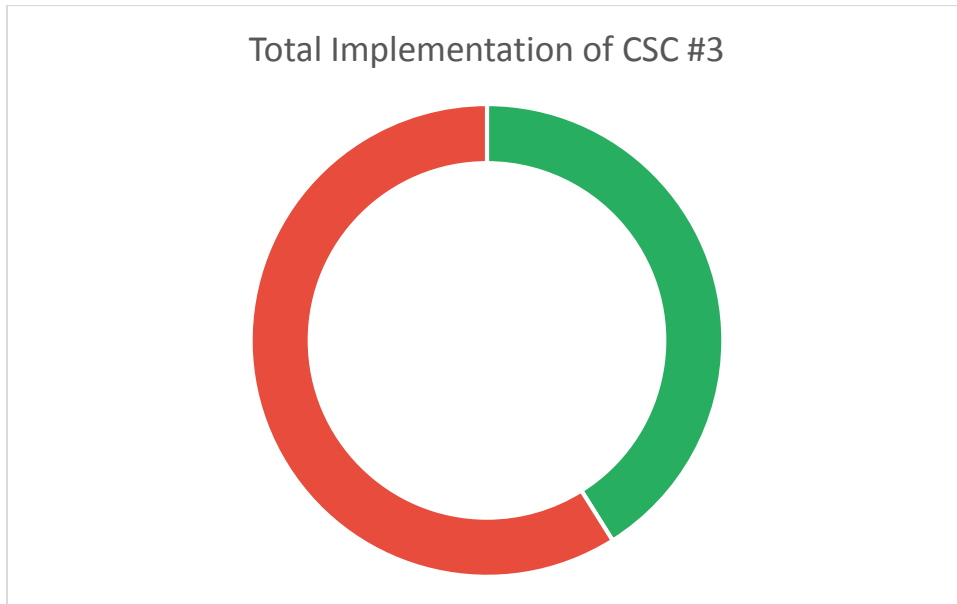
Risk Addressed: 24%

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%

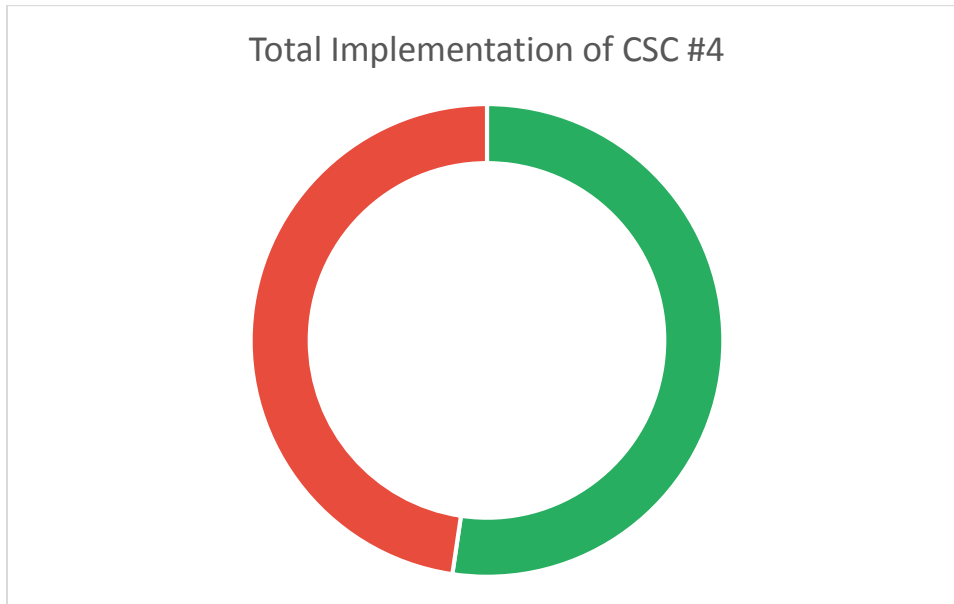
Risk Accepted: 59%

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



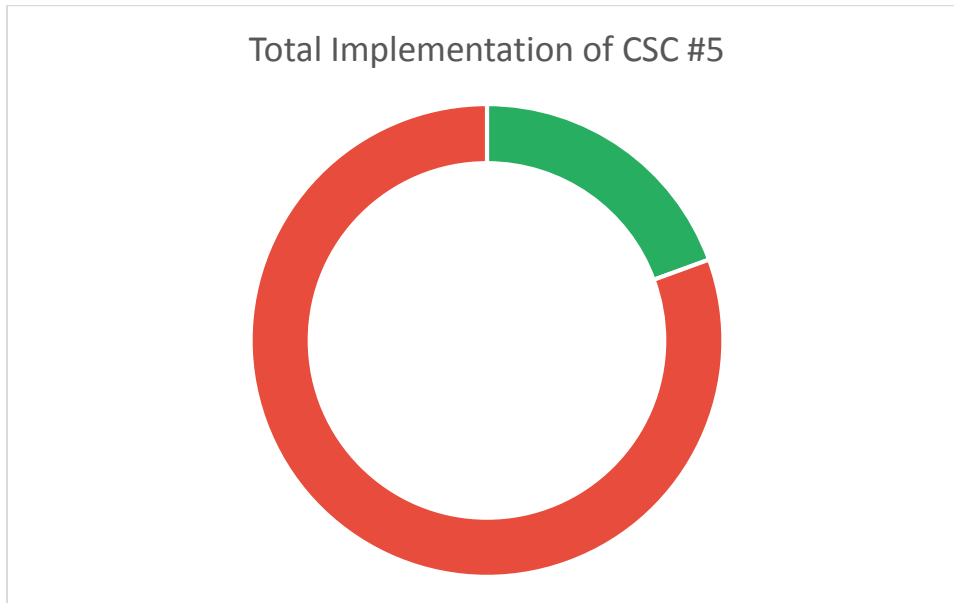
Risk Addressed: 52%

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



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/