University of Idaho

AGRICULTURAL RESEARCH & EXTENSION SERVICE

STRATEGIC PLAN 2021-2025

COLLEGE OF AGRICULTURAL AND LIFE SCIENCES
Agricultural Research and Extension Service
Strategic Plan
2021-2025

MISSION STATEMENT

The College of Agricultural and Life Sciences fulfills the intent and purpose of the land-grant mission and serves the 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 education and life-long learning to become leaders and contributing members of society,
- by fostering healthy populations as individuals and as a society,
- by supporting a vibrant economy, benefiting the individual, families and society as a whole.

VALUES STATEMENT

The College of Agricultural and Life Sciences values:

- excellence in creative discovery, instruction and outreach,
- open communication and innovation,
- individual and institutional accountability,
- integrity and ethical conduct,
- accomplishment through teamwork and partnership,
- responsiveness and flexibility,
- individual and institutional health and happiness.

VISION STATEMENT

We will be the recognized state-wide leader and innovator in meeting current and future challenges to support healthy individuals, families and communities, and enhance sustainable food systems. We will be respected regionally and nationally 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.

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 a culture of collaboration that increases scholarly and creative productivity through interdisciplinary, regional, national and global partnerships.

Performance Measures:

I. Number of grant proposals submitted per year, number of grant awards received per year, and amount of grant funding received per year.
Benchmark: An annual increase of 8% in funding received through both an increase in submissions (350) and awards (300) to reach $27 million in research expenditures by 2024[1].

[1] To attain the University of Idaho's goal of $135 million in research expenditures by 2024, AERS will need to increase grant funding by 8% annually to maintain the college's current proportion of university research expenditures at 20%. The number of grants submitted and received is an increase of 8% and 25%, respectively, over the average of the past 4 years.

Objective B: Create, validate and apply knowledge through the co-production of scholarly and creative works by students, staff, faculty and diverse external partners.

Performance Measures:

I. Number of graduate students (PhD only).
Benchmark: Increase the number of graduate students to 60 by 2024[2].

II. Number of technical publications generated/revised.
Benchmark: Increase the number of technical publications to 240 by 2024[3].

GOAL 2

Engage: Suggest and influence change that addresses societal needs and global issues, and advances economic development and culture.

Objective A: Inventory and continuously assess engagement programs and select new opportunities and methods that provide solutions for societal or global issues, support economic drivers and/or promote the advancement of culture.

Performance Measures:

I. Number of individuals/families benefiting from Outreach Programs.
Benchmark: Increase the number of individuals/families benefiting from Outreach Programs to 430,000 by 2024[4].

II. Number of Youth Participating in 4-H
Benchmark: 75,000 participants in 4-H[5]

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.
- 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.
- Maintenance and replacement of ageing infrastructure continues to impact research and extension productivity. Finding resources to meet these needs is imperative.

[2] To attain the University of Idaho's goal of 380 by 2024, AERS will need to increase the number of graduate students (PhD students only) to 60 to maintain the college's current proportion of university graduate students at 16%.

[3] To attain the goal of 240 technical publications, AERS will need to increase output of 5% annually over the average output for the past 4 years.

[4] To attain the University of Idaho Extension goal of 430,000 by 2024, AERS will need to increase the direct teaching contacts by an average of 6% over the contacts for the past year.

[5] To attain the goal of 75,000 youth participating in 4-H by 2024, AERS will need to increase by 4.4% annually over the average participation for the past 4 years.

Evaluation Process

The Dean's Advisory Board with stakeholders and representatives from agencies in Idaho meets twice annually to review goals and performance of Agricultural Research and Extension. In addition, units (academic departments and extension districts) within the College of Agricultural and Life Sciences also have advisory boards that provide feedback toward those individual unit strategic plans and the performance toward those goals. All of the plans fit under the University of Idaho's Strategic Plan.

Red Tape Reduction Act

The State Board of Education, through the Office of the State Board of Education, runs all administrative rules governing the postsecondary institutions and special and health programs. The State Board of Education strategic plan outlines the reduction efforts for the public education system.

Information Security Overview and Critical Security Controls Assessment Report

Date: March 5, 2020

Status: FINAL

Author: Mitch Parks mitch@uidaho.edu

TLP: GREEN

Contents

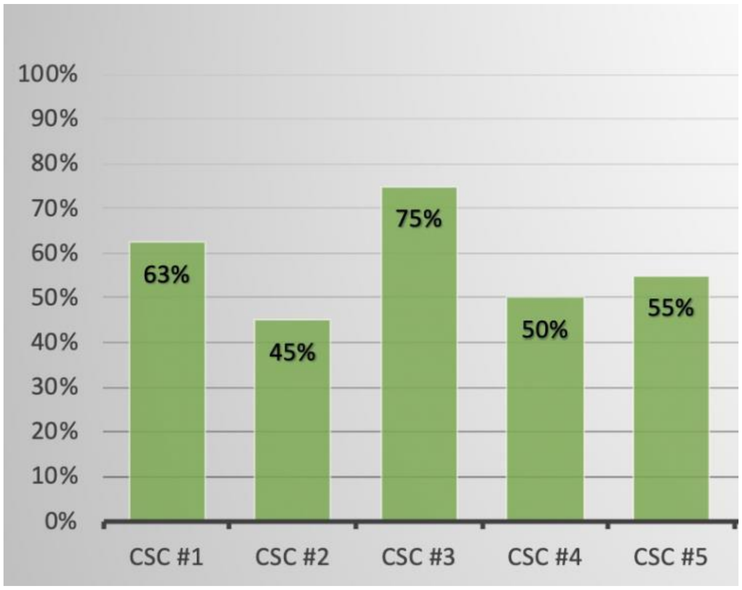
Executive Summary

In response to the Idaho Governor's Executive Order 2017-02 issued January 16, 2017, UI ITS personnel initiated an assessment of the Center for Internet Security (CIS) Critical Security Controls (CSC) 1-5. This assessment was scored using the AuditScripts assessment tool recommended in 2018 by the State Office of the CIO. We continue to regularly re-assess our posture against the CSC using this tool.

Version 7.0 of the Critical Security Controls was released in early 2018. ITS last assessed our status in March 2020 based upon progress implementing controls. That assessment shows an increase from 0.39 to 0.56 (out of 1.0) for overall implementation of the first 5 controls. Between April 2018 and March 2019, our score increased from 0.48 to 0.50, and again to 0.56 by March 2020.

Our Maturity Rating for all 20 controls was improved from 2.00 to 2.45 (out of 5.0) between March 2019 and March 2020.

CSC Version 7 – March 2020



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 are regularly assessed and prioritized.

In 2019, several improvements to controls and mitigations were planned as a result of annual security risk assessment. These risks were prioritized according to the IT Security Plan and utilizing the NIST Cybersecurity Framework (CSF). These mitigations include, but were not limited to:

1. Funding was requested and approved through the University Budget and Finance Committee (UBFC) to enhance email filtering technologies. This was implemented in 2019. CSF: PROTECT

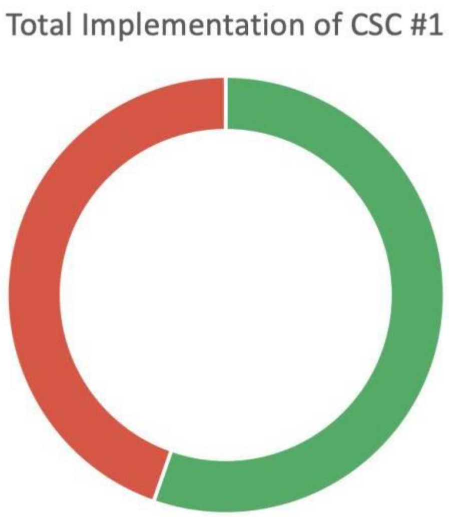
2. Funding was requested and approved through the UBFC to find and mitigate sensitive Personally Identifiable Information on university laptops and desktops (data leakage protection, or DLP). *This project was put on hold indefinitely due to budget reductions*. CSF: DETECT
3. Funding requested through the UBFC to enhance multiple aspects of CSC 1-5, including vulnerability scanning, application whitelisting, security orchestration automation and response, and minimizing administrator privileges. *This was not funded after multiple UBFC requests, but enhanced vulnerability scanning is currently being implemented for high risk areas, using internal ITS funding*. CSF: PROTECT CSF: DETECT
4. Funding requested through the UBFC to implement Network Intrusion Prevention technology, including capability to detect and block malicious activity as a core and fundamental capability. *This has not yet been funded*. CSF: PROTECT CSF: DETECT
5. Funding was requested through the UBFC to implement a system to improve our IT Risk Assessment process and ability to cross-reference our various compliance needs across the institution. *This has not yet been approved or funded.* CSF: IDENTIFY

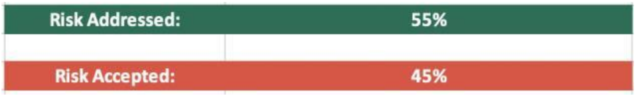
Risks identified against the updated CSC version 7 baseline will again be prioritized in the 2020 IT Security Risk Assessment and mitigations, where feasible or funded, will be addressed within the FY21 IT Security Plan. This will continue to move us towards our target profile under the NIST Cybersecurity Framework.

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 and Control of Hardware Assets



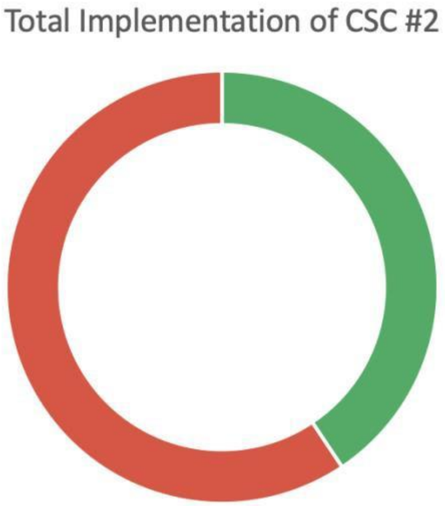


Risk Addressed:	55%
Risk Accepted:	45%

ID	Critical Security Control Detail
1.1	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1.2	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
1.3	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
1.4	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
1.5	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
1.6	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.

1.7	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
1.8	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

CSC #2: Inventory and Control of Software Assets



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

ID	Critical Security Control Detail
2.1	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.
2.2	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventorysystem.
2.3	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
2.4	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.

2.5 The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

2.6 Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

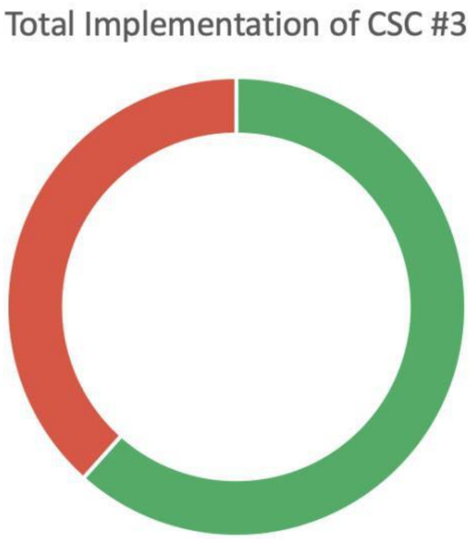
2.7 Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

2.8 The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.

2.9 The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.

2.10 Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.

CSC #3: Continuous Vulnerability Management



Risk Addressed:	62%
Risk Accepted:	38%

ID	Critical Security Control Detail

3.1 Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.

3.2 Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.

3.3 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.

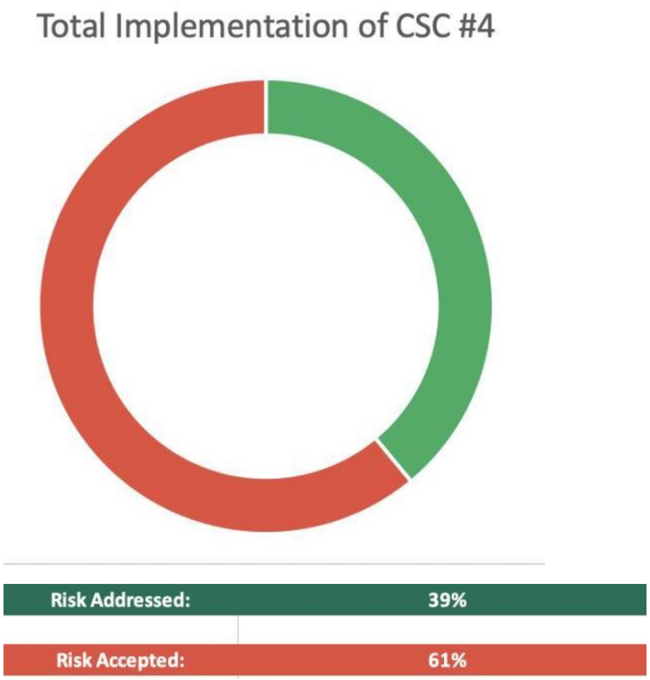
3.4 Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

3.6 Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

3.7 Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

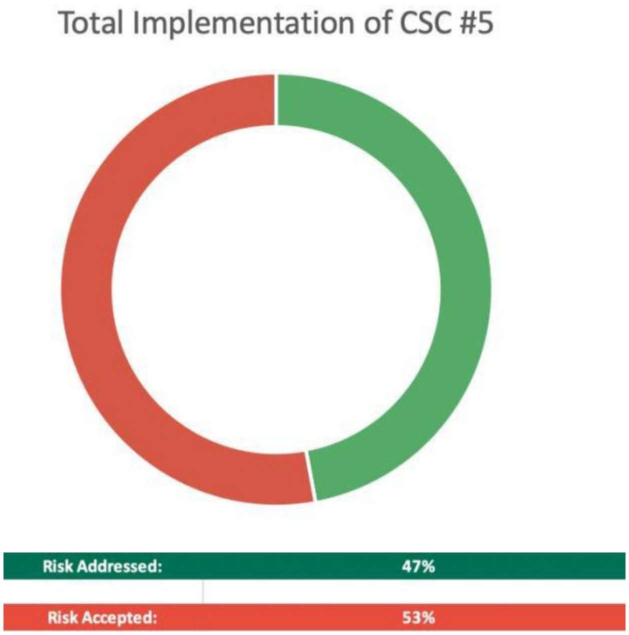
CSC #4: Controlled Use of Administrative Privileges



ID	Critical Security Control Detail
4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
4.2	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
4.3	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
4.4	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
4.5	Use multi-factor authentication and encrypted channels for all administrative account access.
4.6	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
4.7	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.
4.8	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.

4.9	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

CSC #5: Secure Configuration for Hardware and Software



ID	Critical Security Control Detail
5.1	Maintain documented, standard security configuration standards for all authorized operating systems and software.
5.2	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
5.3	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
5.4	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

5.5 Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

Appendix A: References

Tracking of key references useful for this report.

Executive Order 2017-01	Findings of the Idaho Cybersecurity Taskforce	https://adminrules.idaho.gov/bulletin/2017/02.pdf#page=20
Critical Security Controls	Version 7	https://www.cisecurity.org/controls/
Audit Scripts	Free Assessment Resources	http://www.auditscripts.com/free-resources/critical-security-controls/
Policies	U of I IT Policies	https://www.uidaho.edu/governance/policy/policies/apm/30
Standards	IT Standards	https://www.uidaho.edu/its/standards
Privacy	U of I Privacy Statement	https://www.uidaho.edu/privacy
IR Plan	Technology Security Incident Response Plan v1.4	On file