University of Idaho Forest Utilization Research and Outreach (FUR)

STRATEGIC PLAN

FY2021-FY2025

Forest Utilization Research and Outreach (FUR)

MISSION STATEMENT

The Forest Utilization Research and Outreach (FUR) program is located in the College of Natural Resources at The University of Idaho. Its purpose is to increase the productivity of Idaho's forests and rangelands by developing, analyzing, and demonstrating methods to improve land management and related problems such as post-wildfire rehabilitation using state-of-the-art forest and rangeland regeneration and restoration techniques. Other focal areas include sustainable forest harvesting and livestock grazing practices, including air and water quality protection, as well as improved nursery management practices, increased wood use, and enhanced wood utilization technologies for bioenergy and bioproducts. The program also assesses forest products markets and opportunities for expansion, the economic impacts of forest and rangeland management activities, and the importance of resource-based industries to communities and the state's economic development. In addition the Policy Analysis Group follows a legislative mandate to provide unbiased factual and timely information on natural resources issues facing Idaho's decision makers. Through collaboration and consultation FUR programs promote the application of science and technology to support sustainable lifestyles and civic infrastructures of Idaho's communities in an increasingly interdependent and competitive global setting.

VISION STATEMENT

The scholarly, creative, and educational activities related to and supported by Forest Utilization Research and Outreach (FUR) programs will lead to improved capabilities in Idaho's workforce to address critical natural resource issues by producing and applying new knowledge and developing leaders for land management organizations concerned with sustainable forest and rangeland management, including fire science and management, and a full spectrum of forest and rangeland ecosystem services and products. This work will be shaped by a passion to integrate scientific knowledge with natural resource management practices. All FUR programs will promote collaborative learning partnerships across organizational boundaries such as governments and private sector enterprises, as well as landowner and non-governmental organizations with interests in sustainable forest and rangeland management. In addition, FUR programs will catalyze entrepreneurial innovation that will enhance stewardship of Idaho's forest and rangelands, natural resources, and environmental quality.

AUTHORITY and SCOPE

The Forest Utilization Research (FUR) program is authorized by Idaho Statute to enhance the value and understanding of vital natural resources and associated industry sectors via the Policy Analysis Group, Rangeland Center, Experimental Forest and Forest and Seedling Nursery through research, education and outreach to legislators, industry and the Idaho citizenry.

GOAL 1: Scholarship and Creativity

Achieve excellence in scholarship and creative activity through an institutional culture that values and promotes strong academic areas and interdisciplinary collaboration.

Objective A: *Promote an environment that increases faculty, student, and constituency engagement in disciplinary and interdisciplinary scholarship.*

Performance Measures:

I. Number of CNR faculty, staff, students and constituency groups involved in FUR-related scholarship or capacity building activities.

Benchmark: *Number of CNR faculty, staff, students and constituency groups involved in FUR-related scholarship or capacity building activities.*[1] (BY FY2024)

II. ***Number and diversity of courses that use full or partially FUR funded projects, facilities or equipment to educate, undergraduate, graduate and professional students.***

Benchmark: *Number of courses using FUR funded projects, facilities or equipment during instruction.*[2] (BY FY2024)

Objective B: *Emphasize scholarly and creative outputs that reflect our research-extension and land-grant missions, the university and college's strategic themes, and stakeholder needs, especially when they directly support our academic programming in natural resources.*

Performance Measures:

I. ***An accounting of products (e.g., research reports, economic analyses, BMPs) and services (e.g., protocols for new species shared with stakeholders, policy education programs and materials provided, accessible data bases or market models).***

Benchmark: *Numbers and types of products and services delivered and stakeholders serviced.*[3] (BY FY2024)

II. ***An accounting of projects recognized and given credibility by external reviewers through licensing, patenting, publishing in refereed journals, etc.***

Benchmark: *Number of peer reviewed reports and referred articles produced using FUR funding, facilities or equipment.*[4] (BY FY2024)

GOAL 2: Outreach and Engagement

Engage with the public, private and non-profit sectors through mutually beneficial partnerships that enhance teaching, learning, discovery, and creativity.

Objective A: *Build upon, strengthen, and connect the College of Natural Resources with other parts of the University to engage in mutually beneficial partnerships with stakeholders to address areas targeted in FUR.*

Performance Measures:

I. ***Document cases: Communities served and resulting documentable impact; Governmental agencies served and resulting documentable impact; Non-governmental agencies served and resulting documentable impact; Private businesses served and resulting documentable impact; and Private landowners served and resulting documentable impact. Meeting target numbers for audiences identified below and identifying mechanisms to measure economic and social impacts.***

Benchmark: Number of external participants served.[5] (BY FY2024)

GOAL 3: Financial Efficiency and Return on Investment (ROI)

Efficient financial management of FUR state appropriated dollars supporting Goals 1 and 2 and leveraging resources to secure external funding (e.g., external grants, private funding, and cooperatives)

Objective A: *Leveraging state funds to secure additional financial resources to increase impact on products, services and deliverables.*

Performance Measures:

I. ***New funding sources from external granting agencies, private and public partnerships and other funding groups.***

Baseline data/Actuals:

Benchmark: *Number of new research projects leveraged using external funding.*[6] (BY FY2024)

Key External Factors

The key external factors likely to affect the ability of FUR programs to fulfill the mission and goals are as follows: (1) the availability of funding from external sources to leverage state-provided FUR funding; (2) changes in human resources due to retirements or employees relocating due to better employment opportunities; (3) continued uncertainty relative to global, national and regional economic conditions; and (4) changing demand for the state and region's ecosystem services and products.

Evaluation Process

Quarterly status meetings between FUR units, including PAG, Rangeland Center, Experimental Forest and Research Nursery to ensure coordinated work, identification of new opportunities, and projects. Assessment of external proposals and new funding sources for leveraging for match opportunities to increase impacts of research, outreach, and technology transfer. Annual review of strategic plan to determine applicable progress toward benchmark and growth.

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.

[1] Increased staff resources in 2016 will allow us to involve more faculty, staff, students and constituency groups in FUR-related scholarship activities.

[2] Based on College and program goals to enhance coordination of course offerings and research.

[3] Based on critical need to communicate with external stakeholders, and increase the pace of products produced.

[4] Increased staff resources in 2016 focused on research will increase scientific outreach and communication.

[5] New measure based on UI and college strategic goal to increase involvement and communication with external stakeholders. Benchmark established from internal analysis of recent year participants served.

[6] Based on analysis of projects started and completed in recent years, staff capacity, and critical need to increase the pace of projects completed annually

Appendix 1

	State Board of Educa		
	Goal 1: A WELL EDUCATED CITIZENRY	*Goal 2: INNOVATION AND ECONOMIC DEVELOPMENT*	*Goal 3: DATA-INFORMED DECIS MAKING*
Institution/Agency Goals and Objectives			
GOAL 1: SCHOLARSHIP and CREATIVITY ***Achieve excellence in scholarship and creative activity through an institutional culture that values and promotes strong academic areas and interdisciplinary collaboration.***			
Objective A: Promote an environment that increases faculty, student, and constituency engagement in disciplinary and interdisciplinary scholarship	✓		✓
Objective B: Emphasize scholarly and creative outputs that reflect our research-extensive and land-grant missions, the university and college's strategic themes, and stakeholder needs, especially when they directly support our academic programming in natural resources.	✓	✓	✓
GOAL 2: OUTREACH and ENGAGEMENT ***Engage with the public, private and non-profit sectors through mutually beneficial partnerships that enhance teaching, learning, discovery, and creativity.***			
Objective A: Build upon, strengthen, and connect the College of Natural Resources with other parts of the University to engage in mutually beneficial partnerships with stakeholders to address areas targeted in FUR.			
GOAL 3: FINANCIAL EFFICIENCY and RETURN ON INVESTMENT ***Efficient financial management of FUR state appropriated dollars supporting Goals 1 and 2 and leveraging resources to secure external funding (e.g., external grants, private funding, and cooperatives)***			
Objective A: Leveraging state funds to secure additional financial resources to increase impact on products, services and deliverables.		✓	✓

Information Security Overview and Critical Security Controls Assessment Report

Date: March 5, 2020

Status: FINAL

Author: Mitch Parks mitch@uidaho.edu

TLP: GREEN

Contents

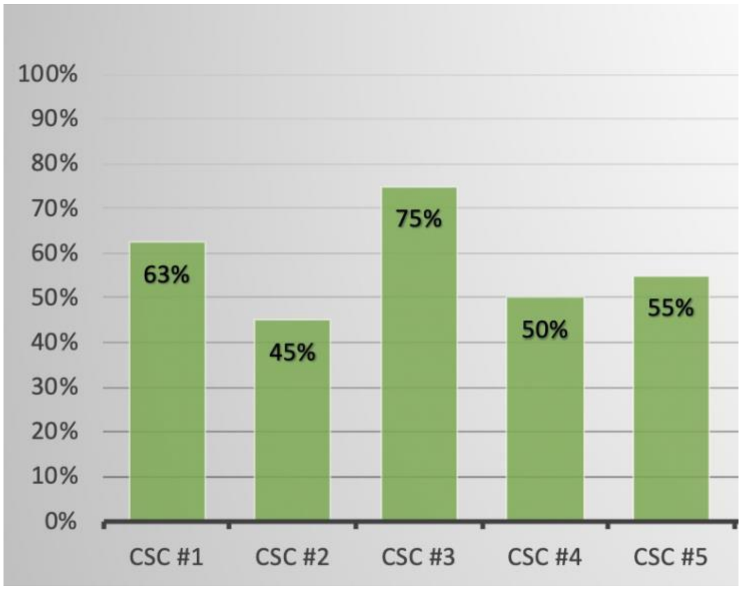
Executive Summary

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

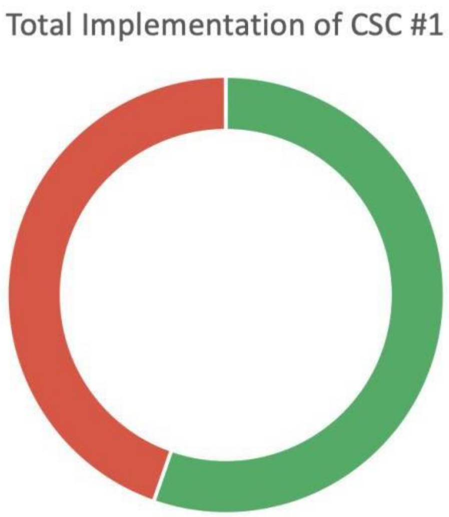
2. Funding was requested and approved through the UBFC to find and mitigate sensitive Personally Identifiable Information on university laptops and desktops (data leakage protection, or DLP). *This project was put on hold indefinitely due to budget reductions*. CSF: DETECT
3. Funding requested through 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

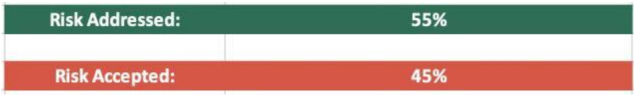
Risks identified against the updated CSC version 7 baseline will again be prioritized in the 2020 IT Security Risk Assessment and mitigations, where feasible or funded, will be addressed within the FY21 IT Security Plan. This will continue to move us towards our target profile under the NIST Cybersecurity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



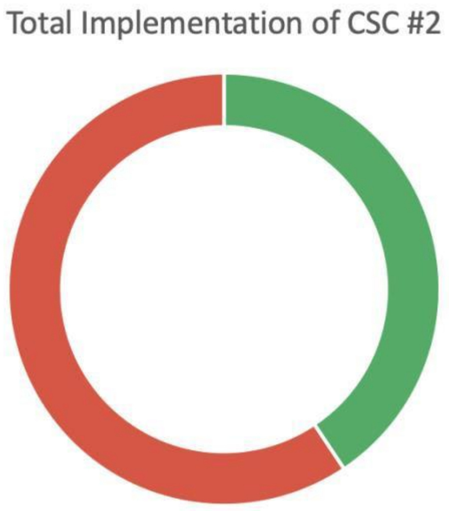


Risk Addressed:	55%
Risk Accepted:	45%

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

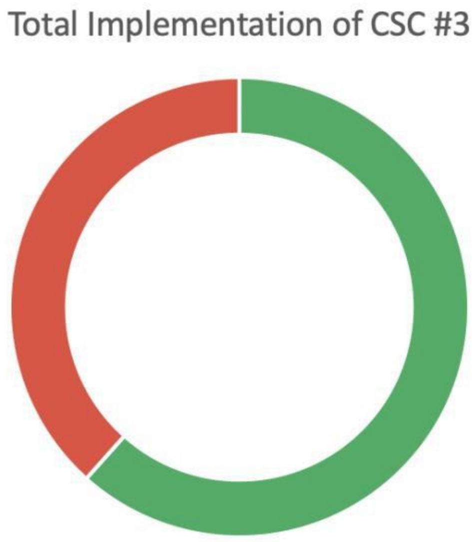


Risk Addressed:	**41%**
Risk Accepted:	**59%**

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.

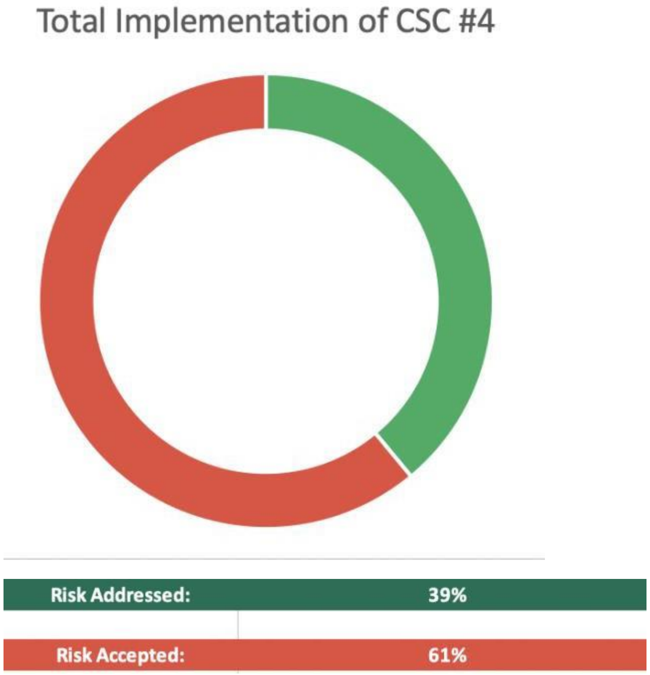
3.4 Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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

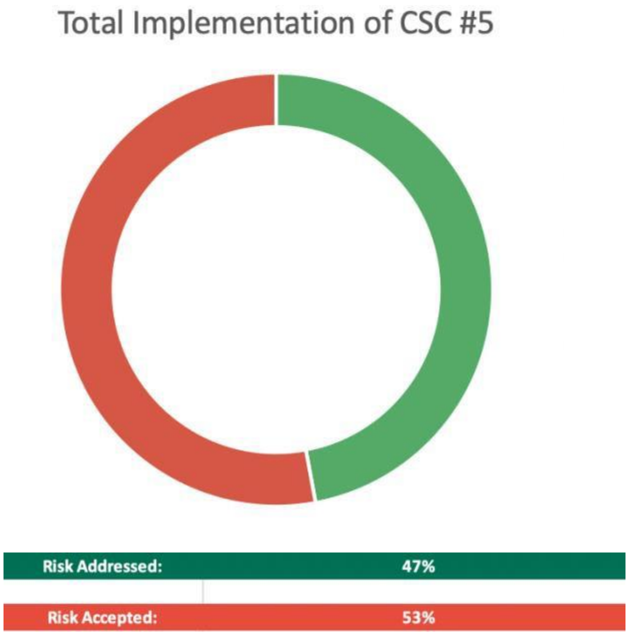


Risk Addressed:	39%
Risk Accepted:	61%

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