IDAHO
GEOLOGICAL SURVEY

University of Idaho

STRATEGIC PLAN
FY2021 - FY2025

The Idaho Geological Survey (IGS) is a non-regulatory state agency that leads in the collection, interpretation, and dissemination of geologic and mineral data for Idaho. The agency has served the state since 1919 and prior to 1984 was named the Idaho Bureau of Mines and Geology.

MISSION STATEMENT

The Survey's mission is to provide the state with timely and relevant geologic information. Members of the IGS fulfill this mission through applied geologic research and strong collaborations with federal and state agencies, academia, and the private sector. IGS research focuses on geologic mapping, geologic hazards (earthquakes and landslides), hydrogeology (surface and groundwater evaluation), geothermal energy, oil and gas, and metallic and industrial minerals. The Survey's Digital Mapping Laboratory is central to compiling, producing, and delivering new digital geologic maps and publications for the agency. The IGS is also engaged in dissemination of historic mining records, community service, and earth science education. As Idaho grows, demand is increasing for geologic and geospatial information related to energy, mineral, and water resource development, and landslide and earthquake hazards.

VISION STATEMENT

IGS is committed to the advancement of diverse disciplines within the geosciences and emphasizes the practical application of geology to benefit society. The Survey seeks to accomplish its responsibilities through service and outreach, research, and education.

AUTHORITY

Idaho Statutes, Title 47, Chapter 2 provides for the creation, purpose, duties, reporting, offices, and Advisory Board of the IGS. The Statutes specify the authority to conduct investigations, establish cooperative projects, and seek research funding. The IGS publishes an Annual Report as required by its enabling act.

GOAL 1: Service and Outreach

Achieve excellence in collecting and disseminating geologic information and mineral data to the public, governmental agencies, elected officials, educational institutions, civic and professional organizations, and the mining, energy, agriculture, utility, construction, insurance and banking industries. Continue to strive for increased efficiency and access to survey information primarily through publications, website products, in-house collections, and customer inquiries. Emphasize website delivery of digital products and compliance with new revision of state documents requirements (Idaho Statute 33-2505).

Objective A: Develop and publish survey documents

Initiate and develop research initiatives and publish geological maps, technical reports, and data sets.

Performance Measures:

I. **Number of Published Reports on Geology/Hydrogeology/Geohazards/Mineral & Energy Resources.**

Benchmark: The number and scope of published reports will be equal to or greater than the last full fiscal year reported, given comparable scope and staffing levels.[1]

Objective B: Deliver statewide geologic information and products via website
Create and deliver IGS products and publications to the general public, state and federal agencies, and cooperators in an efficient and timely manner. Products include GIS data sets, reports, map publications, and web map applications.

Performance Measures:

I. **Number of website viewers.**
Benchmark: The number of website viewers (excluding robot searches) will be equal to or greater than the last full fiscal year reported.[1]

II. **Number of website products used or downloaded.**
Benchmark: The number of website products used or downloaded will be equal to or greater than the last full fiscal year reported.[1]

Objective C: Sustain Idaho State Documents Depository Program and Georef Catalog (International)
Deliver all IGS products and publications to the Idaho Commission for Libraries for cataloging and distribution to special document collections in state university libraries and deliver digital copies of all products and publications to GeoRef for entry in their international catalog of geologic literature.

Performance Measures:

I. **Percentage of Survey documents available through these programs.**
Benchmark: All newly published IGS documents will be made available through these programs [4]

Objective D: Sustain voluntary compliance
Sustain voluntary compliance with uploads of new geologic mapping products published at the Idaho Geologic Survey to the National Geologic Map Database Website managed by the U.S. Geological Survey.

Performance Measures:

I. **Percentage of published Geologic Maps that are uploaded to the national website depicting detailed geologic mapping in Idaho.**
Benchmark: All geologic maps that are published at the IGS each year will be uploaded to this website.[4]

GOAL 2: Research
Promote, foster, and sustain a climate for research excellence. Develop existing competitive strengths in geological expertise. Maintain national level recognition and research competitiveness in digital geological mapping and applied research activities. Sustain and build a strong research program through interdisciplinary collaboration with academic institutions, state and federal land management agencies, and industry partners.

Objective A: Sustain and enhance geological mapping
Sustain and enhance geological mapping and study areas of particular interest including those with economic potential and geohazard concerns.

Performance Measures:

I. **Increase the geologic map coverage of Idaho by mapping priority areas of socioeconomic importance. Identify and study areas with geologic resources of economic importance and identify and study areas that are predisposed to geologic hazards.[5]**
Benchmark: Increase the cumulative percentage of Idaho's area covered by modern geologic mapping.[6]

Objective B: Sustain and build external research funding
Sustain existing state and federal funding sources to maintain research objectives for the IGS. Develop new

sources of funding from private entities such as oil and gas, mining, and geothermal energy companies that are exploring and developing geologic resources in Idaho.

__Performance Measures:__

I. **Increase externally funded grant and contract dollars with a focus of securing new sources of funding from the private sector.**
   Benchmark: Increase externally funded grant and contract dollars compared to five-year average.[6]

GOAL 3: Education

Support knowledge and understanding of Idaho's geologic setting and resources through earth science education. Achieve excellence in scholarly and creative activities through collaboration and building partnerships that enhance teaching, discovery, and lifelong learning.

__Objective A: Provide earth science education__

Develop and deliver earth science education programs, materials, and presentations to public and private schools.

__Performance Measures:__

I. **Number of educational programs provided to public and private schools and the public at large.**
   Benchmark: The number of educational and public presentations will be equal to or greater than the last full fiscal year reported.[7]

Key External Factors Funding:

Achievement of strategic goals and objectives is dependent on appropriate state funding.

External research support is partially subject to competitive federal funding, and some federal programs require a state match.

Consistent state funding is critical given the Survey's commitments to provide deliverables that include digital geologic maps, reports on mineral exploration, oil and gas exploration, water resource assessment, and geologic hazards (seismic and slope stability), along with archiving older, unpublished mining records.

With the assistance of the Survey's Advisory Board, we are receiving valuable advice, as we seek partnerships with state and private entities to produce non-proprietary products accessible through the Survey's website.

Demand for services and products:

Changes in demand for geologic information due to energy and mineral economics play an important role in the achievement of strategic goals and objectives. State population growth and requirements for geologic and geospatial information by public decision makers and land managers are also key external factors that are projected to increase over time.

Aspirational Goals for the IGS:

- Increase public outreach and promote the state's resource-based economy.
- Implement an interdisciplinary geologic study of the Treasure Valley region that will connect surface geologic mapping, oil and gas subsurface work, hydrogeology, and hazards.
- Understand the southwest Idaho oil and gas play's source and reservoirs, as well as conduct baseline evaluations of the favorable structures in southern and southeast Idaho.
- Build a functional hazards program that will coordinate with the Idaho Office of Emergency

Management and other agencies to focus on geologic hazard assessments and protection of human lives, homes, and the state's infrastructure such as pipelines, roads, railroads, and dams.

- Coordinate with various surface water and groundwater data collection and administrative agencies to assess watersheds in focus areas of the state and increase outreach and understanding of water resource issues.
- Improve understanding of mineral and ore deposits that are currently being mined and explored including cobalt, phosphate, silver, gold, and rare earth elements.
- Continue to work with the Idaho Geologic Mapping Advisory Committee to develop a 5- to 10- year geologic mapping plan.
- Improve the Survey's website and web map applications to accommodate visualization and interaction through mobile devices for ease of public use.

Evaluation Process

An annual review of existing benchmarks and goals is necessary to ensure that IGS is successfully executing its strategic plan and providing relevant and timely geologic and geospatial information to the public on the Survey's website. New technologies will be continually evaluated on an annual basis to ensure IGS is providing its data and publications in a user-friendly format that is easily accessible to the public.

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.

Cyber Security Plan

As a functional part of the University of Idaho the Idaho Geological Survey is subject to the University of Idaho Cyber Security Plan.

[1] These benchmarks are set based on existing resources and projected increases for this area. No additional resources were projected at the time of setting this benchmark, therefore a minimal increase would indicate growth in this area and increase efficiencies.

[2] Due to the ongoing implementation of a different web statistic tool on our new website, the actual measures may be different than what was reported in the Performance Report, and the benchmark set for FY22 may not be that meaningful.

[3] Due to the ongoing implementation of a different web statistic tool on our new website, the number of website products used or downloaded reported for FY19 reflects only products used or downloaded from the interactive map and does not include publications, databases, or other downloads from our website.

[4] This benchmark is based on current levels of performance and maintaining the current high level.

[5] It was determined percentage of geologic map coverage was calculated incorrectly in the past. Calculations have been corrected here.

[6] This benchmark is dependent in part on the ability to receive external grants to broaden areas not already covered. Due to the increasingly competitive nature of external grant funding it is determined that a simple increase of areas covered was a more meaningful measure than a set number of projects.

[7] This benchmark is based on existing resources (including staff time) to provide presentations and developing educational partnerships to provide new venues for additional presentation above and beyond the current partnerships with public schools and postsecondary institutions.

Information Security Overview and Critical Security Controls Assessment Report

Date: March 5, 2020

Status: FINAL

Author: Mitch Parks mitch@uidaho.edu

TLP: GREEN

Contents

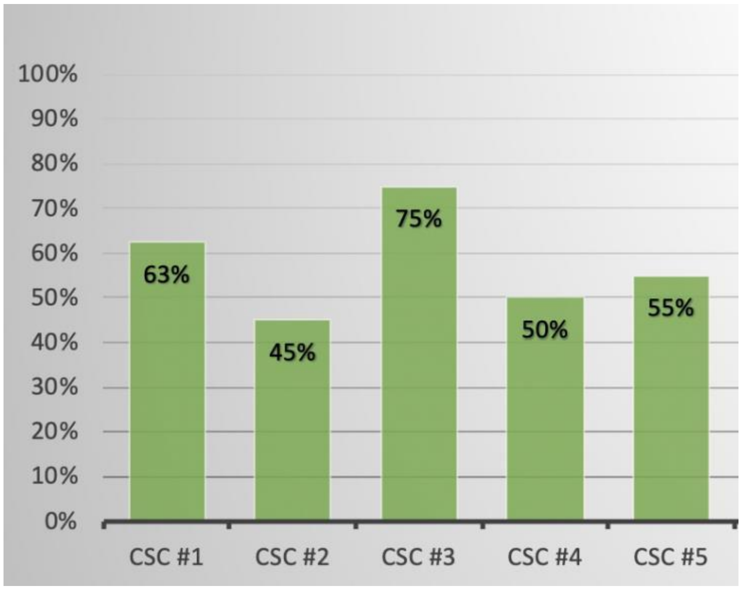
Executive Summary

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

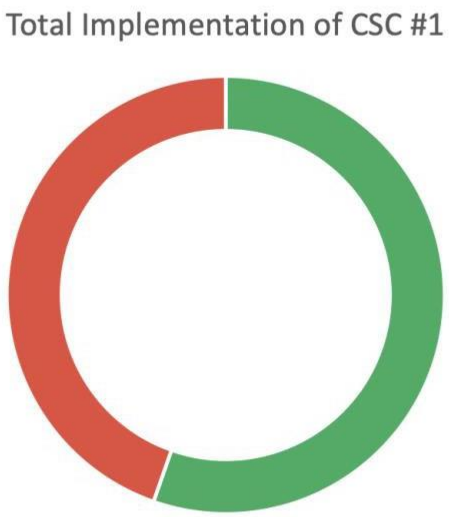
2. Funding was requested and approved through the UBFC to find and mitigate sensitive Personally Identifiable Information on university laptops and desktops (data leakage protection, or DLP). *This project was put on hold indefinitely due to budget reductions*. CSF: DETECT
3. Funding requested through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



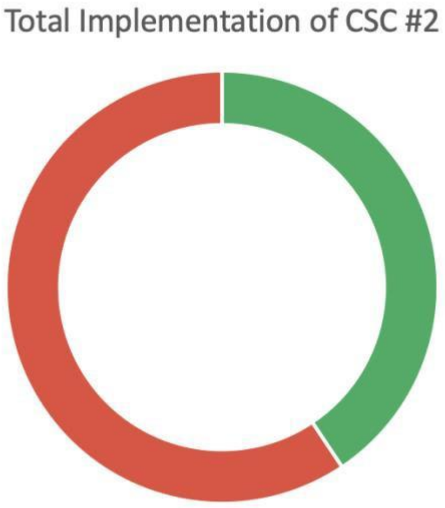
Total Implementation of CSC #1

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


Total Implementation of CSC #2

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.

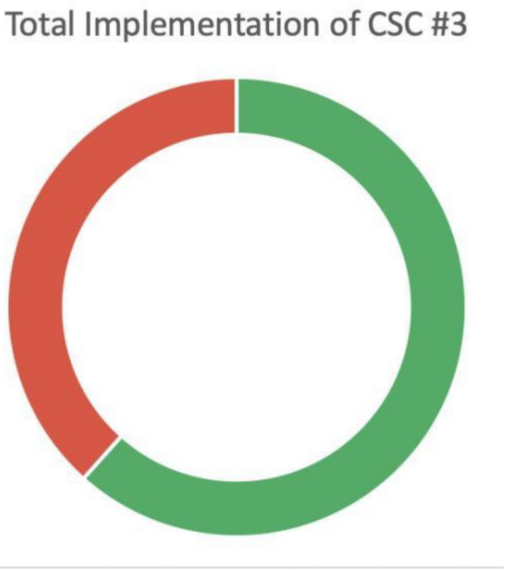
2.7 Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.

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.

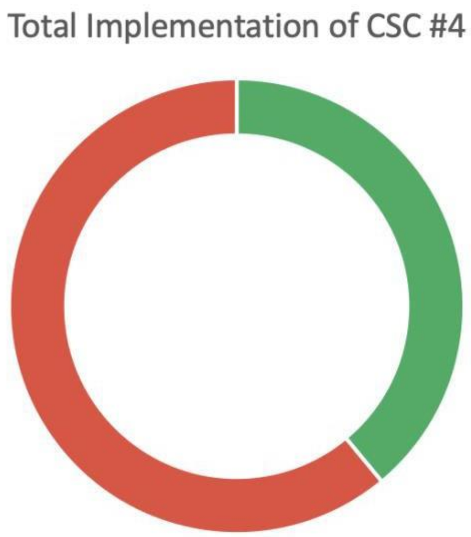
3.4 Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

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

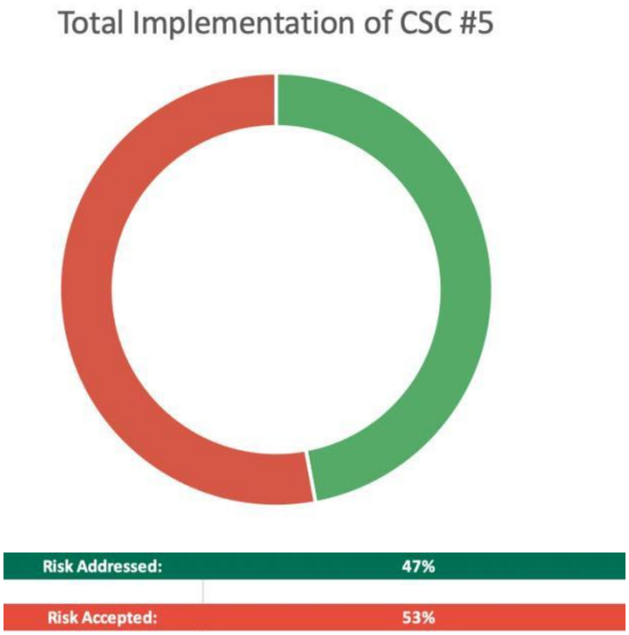


Risk Addressed:	39%
Risk Accepted:	61%

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



Risk Addressed:	47%
Risk Accepted:	53%

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