IDAHO
GEOLOGICAL SURVEY

FY2018-2022 Strategic Plan

MISSION STATEMENT

The Idaho Geological Survey is the lead state agency for 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.

Members of the Idaho Geological Survey staff acquire geologic information through field and laboratory investigations and through cooperative programs with other governmental, academic, and private sector alliances. The Idaho Geological Survey provides timely and meaningful information to the public, industry, academia, and legislative decision makers by conducting geologic mapping, geohazard assessments that focus on earthquakes and landslides, mineral and energy resource assessments, groundwater and hydrology research, and educational and outreach opportunities. The Survey's Digital Mapping Laboratory is central to compiling, producing, and delivering new digital geologic maps and publications for the agency. The Idaho Geological Survey is also engaged in the collection and compilation of data and information pertaining to abandoned and inactive mines in the state, earth science education, and a newly added focus of petroleum geology assessments. As Idaho grows, demand is increasing for geologic and geospatial information related to population growth, energy-mineral and water-resource development, landslide hazards, and earthquake monitoring.

VISION STATEMENT

The Idaho Geological Survey vision is to provide the state with the best geologic information possible through strong and competitive applied research, effective program accomplishments, and transparent access. We are committed to the advancement of the science and emphasize the practical application of geology to benefit society. We seek to accomplish our responsibilities through service and outreach, research, and education.

AUTHORITY

Idaho Code provides for the creation, purpose, duties, reporting, offices, and Advisory Board of the Idaho Geological Survey. The Code specifies the authority to conduct investigations, establish cooperative projects, and seek research funding. The Idaho Geological Survey 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 mining, energy, agriculture, utility, construction, insurance, and banking industries, educational institutions, civic and professional organizations, elected officials, governmental agencies, and the public. 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 Code 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/Hydrology/Geohazards/Mineral & Energy Resources (999 Publications, Maps, and Reports cumulative).**

Baseline data/Actuals:

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
32	**27**	**39**		**39**

Benchmark: The number and scope of published reports will be equal to or greater than the number of publications from the preceding year.[1]

Objective B: Build and deliver website products - Create and deliver Idaho Geological Survey 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 products used or downloaded (For FY16 there were 398,400 visitors to the Idaho Geological Survey website).**

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
132,454	**157,540**	**185,635**		**191,709**

Benchmark: The number of website products used or downloaded will be equal to or greater than the preceding year.[1]

Objective C: Sustain Idaho State Documents Depository Program and Georef Catalog (International) - Deliver all Idaho Geological Survey 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 total of Survey documents available through these programs (~ 99%).**

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
~99%	**~99%**	**~99%**	**~99%**	**100%**

Benchmark: 100%[2]

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. **Number of Geologic Maps that are uploaded to this national website depicting detailed geologic mapping in Idaho (589 maps cumulative have been uploaded).**

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

Benchmark: 100% of all geologic maps that are published at the Idaho Geological Survey each year will be uploaded to this website.[2]

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 that have 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.**

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
36.6	**36.9**	**37.4**		**37.8**

Benchmark: Increase the cumulative percentage of Idaho's area covered by modern geologic mapping. Re-evaluate geologic resources in Idaho that may have economic potential and identify and rank geologic hazards throughout the state.[3]

Objective B: Sustain and build external research funding – Sustain existing state and federal funding sources to maintain research objectives for the Idaho Geological Survey. 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 particular focus of securing new sources of funding from the private sector.**

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
$371,023	**$382,101**	**$498,034**		**$457,794**

Benchmark: The number of externally funded grant and contract dollars compared to five year average.[3]

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.**

FY14 (2013-2014)	**FY15** (2014-2015)	**FY16** (2015-2016)	**FY17** (2016-2017)	**Benchmark**
20	**9**	**19**		**≥ 19**

Benchmark: The number of educational and public presentations will be equal to or greater than the previous year.[4]

Key External Factors

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

External research support is partially subject to federal funding, and there is increasing state competition for federal programs. Because most federal programs require a state match, the capability to secure these grants is dependent on state funds and the number of full time equivalent employees.

Emerging natural gas and condensate infrastructure and production in southwestern Idaho will necessitate new research tools and personnel at the Survey to maintain research capabilities and to provide pertinent information to the public and the Idaho legislature. Economic and research partnerships with the oil and gas industry have been secured during the past year.

New partnerships are also being sought through universities, state and federal agencies, and natural resource industries.

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. Over the past six years, Idaho Geological Survey has experienced an 82% increase in the number of downloaded products from the Survey's website. The number of visitors to the Idaho Geological Survey website has increased by 87% over the same six year time frame. 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 Idaho Geological Survey:
Provide critical mass for primary customer services in southern and central Idaho through consolidation of personnel and technical resources at the Idaho Water Center in Boise. Appointment of new geological staff and support personnel to the Boise office of Idaho Geological Survey will permit a more responsive agency in southern and central Idaho and better coordination with other state agencies at the state's capitol.

Provide high quality petroleum assessments and geologic services to evaluate regions of existing oil and gas production and investigate other perspective areas in Idaho that have potential for developing hydrocarbon resources.

A multi-agency legislative request for one-time funding to build a permanent facility in the Boise metro region to house exploration drill cores and well cuttings. The purpose of the facility is to capture hundreds of millions of dollars of valuable and perishable subsurface information through the storage of geologic samples associated with oil and gas, mineral, geothermal, and groundwater exploration activities. Ongoing funding for building maintenance, utilities, and one warehouse technician to catalogue and maintain the samples for public and industry research and viewing is necessary. A legislative request for a small percentage (~0.25%) of the proceeds from oil and gas severance taxes could be a potential source of ongoing funding to address the building maintenance and salary and benefits for the warehouse technician.

Progressive development of personnel and agency resources to build a full-time geologic hazards program stationed in the Boise office of the Idaho Geological Survey that will coordinate with the Idaho Department of Emergency Management and focus on geologic hazard assessments and protection of human lives, homes, and the state's infrastructure such as pipelines, roads, and dams.

Increase the number and scope of digital web applications for the Survey's digital maps, datasets, and geologic information to accommodate smart phone and tablet technologies for the public. Currently 40% of all downloads from the agency website is to personal electronic devices.

Evaluation Process

An annual review of existing benchmarks and goals is necessary to ensure that Idaho Geological Survey is successfully executing its strategic plan and providing relevant and timely geologic and geospatial information for public dissemination. Research opportunities will be continually explored and collaborations with new funding partners, especially in the private sector, will be embraced. New technologies and data capture techniques will be continually evaluated on an annual basis to ensure Idaho Geological Survey is providing its data and publication resources in a user-friendly format that is easily accessible to the public. Ongoing review of regulatory and legal compliance obligations to state, federal, and private funding partners is a necessary requirement to maintain the research capabilities of the Idaho Geological Survey.

---

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

[3] 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.

[4] 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.

Cybersecurity Overview and Critical Security Controls Assessment Report

Date: June 19, 2017

Status: FINAL

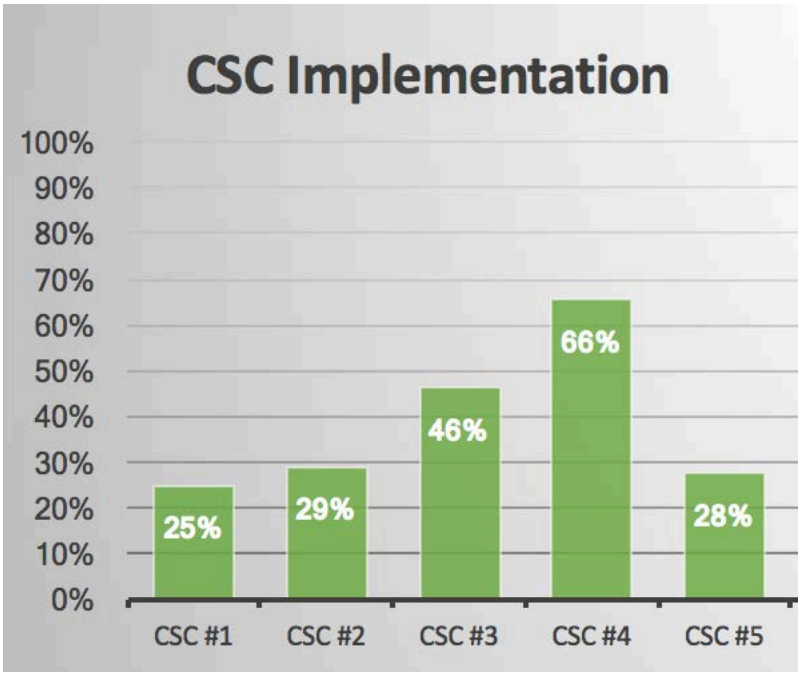
Author: Mitch Parks mitch@uidaho.edu

Contents

Executive Summary

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

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



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

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

High Level Cybersecurity Assessment

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

Policies/Procedures

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

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

External Review

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

Technology Security Advisory Council

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

Employee Training and Awareness

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

Encryption

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

Governor's Executive Order No. 2017-02

Two of the ten directives listed in the EO are:

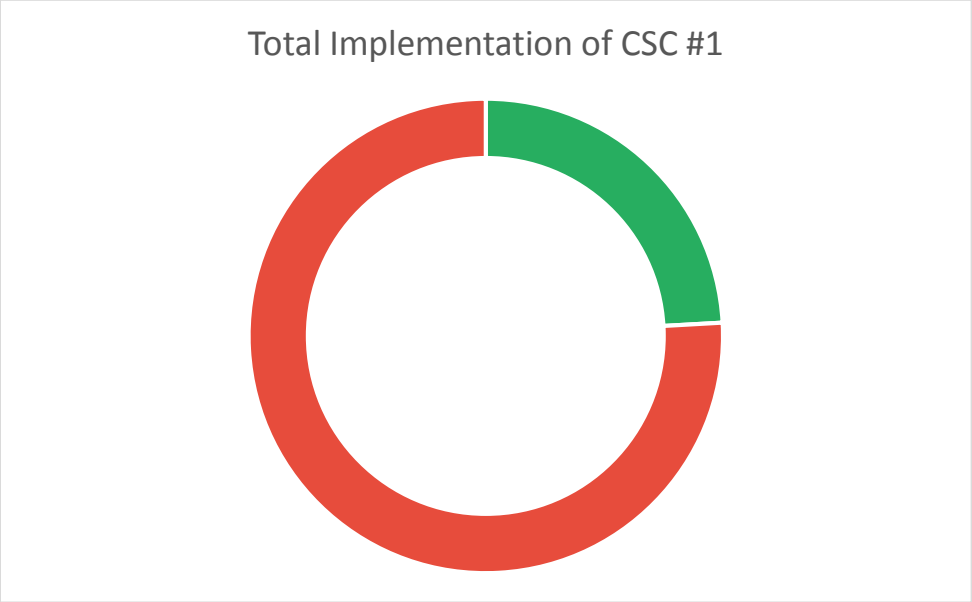
- Adoption and implementation of the National Institute of Standards and Technology (NIST) cybersecurity framework; and
- Implementation of the first five Center for Internet Security (CIS) critical security controls.

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

Critical Security Controls

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

CSC #1: Inventory of Authorized and Unauthorized Devices

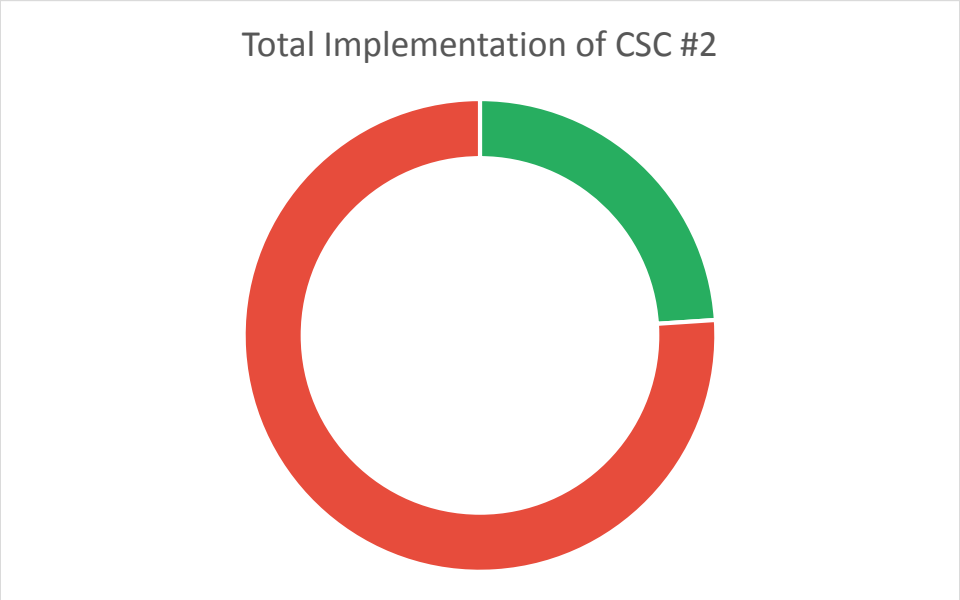


Risk Addressed:	**24%**
Risk Accepted:	**76%**

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

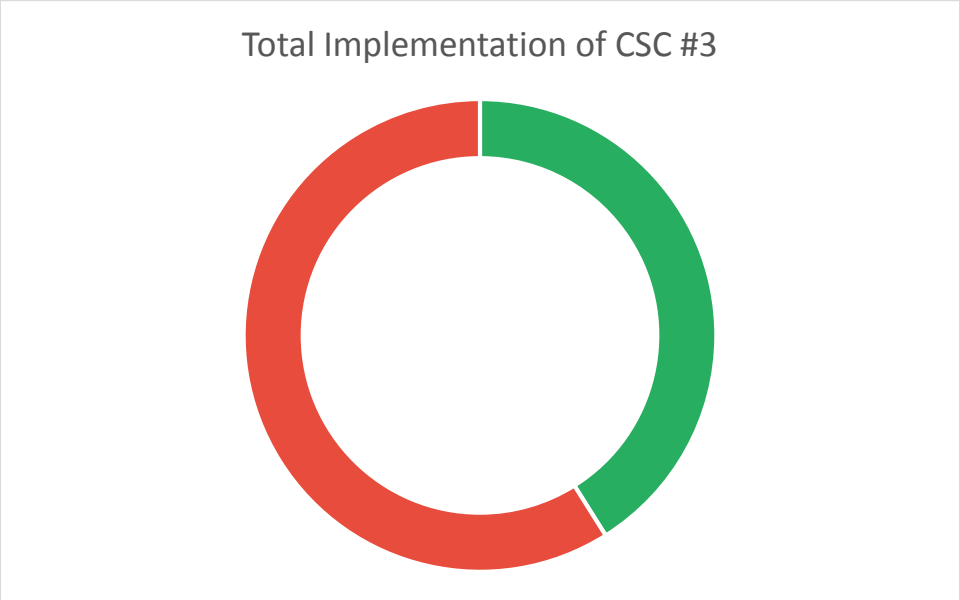


Risk Addressed:	**24%**
Risk Accepted:	**76%**

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



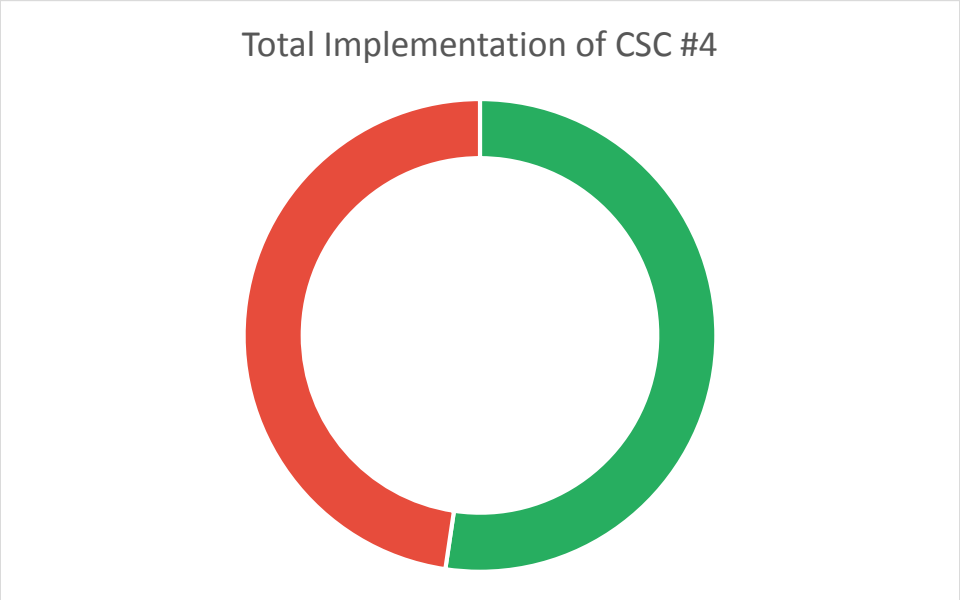
Risk Addressed:	**41%**
Risk Accepted:	**59%**

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

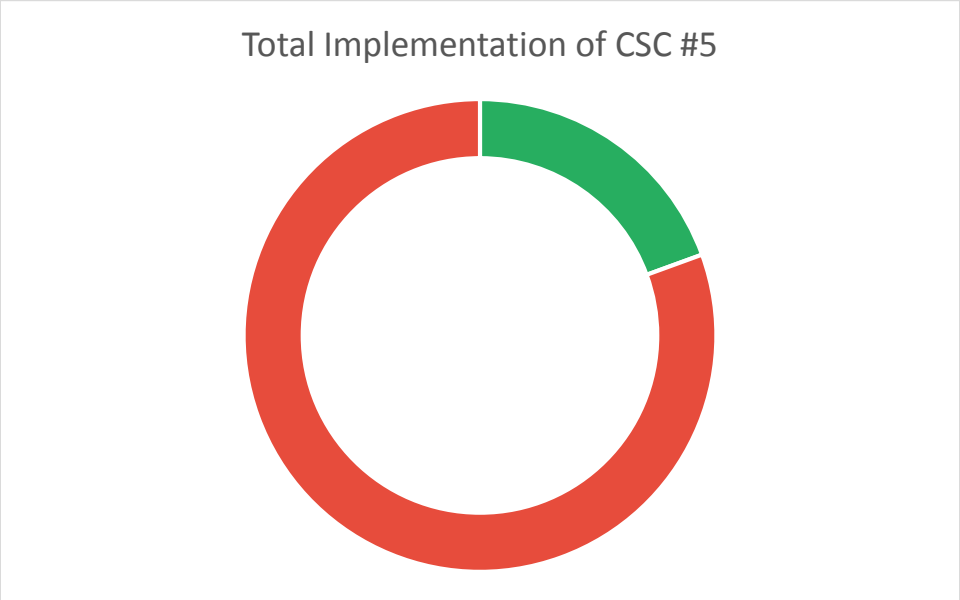


Risk Addressed:	**52%**
Risk Accepted:	**48%**

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/