Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority

Colorado Statewide Internet Portal Authority

Information Technology Performance Evaluation

Public Report

February 2021

Eide Bailly LLC

EideBailly

CPAs & BUSINESS ADVISORS

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Representative Dafna Michaelson Jenet – Chair
Senator Jim Smallwood – Vice Chair
Representative Rod Bockenfeld
Senator Julie Gonzales
Representative Colin Larson
Representative Dylan Roberts
Senator Robert Rodriguez
Senator Rob Woodward

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditor
Eide Bailly LLP	Contractor

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT **WWW.STATE.CO.US/AUDITOR**

A BOUND REPORT MAY BE OBTAINED BY CALLING THE
OFFICE OF THE STATE AUDITOR
303.869.2800

PLEASE REFER TO REPORT NUMBER 2050P-IT WHEN REQUESTING THIS REPORT

EideBailly®

CPAs & BUSINESS ADVISORS

February 2021

Members of the Legislative Audit Committee:

This report contains the results of our Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority. The assessment was conducted pursuant to Section 2-3-103, C.R.S, which authorizes the State Auditor to conduct evaluations and assess the security practices of information technology systems of all department, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Colorado Statewide Internet Portal Authority.

We conducted this engagement as an IT performance evaluation, and although we did not attempt to strictly follow generally accepted government auditing standards, we did obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and recommendations based on the evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

During our evaluation work, we identified certain matters that are not included in this evaluation report that were reported to the Colorado Statewide Internet Portal Authority in a separate confidential report dated February 2021. These matters were considered sensitive in order to protect state information technology assets.

E. Anders Erickson
Principal
Eide Bailly, LLC

CONTENTS

REPORT HIGHLIGHTS

Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority

Involved assessment of the security of web applications and supporting systems and processes at the Colorado Statewide Internet Portal Authority (SIPA).

Information Technology Performance Evaluation, 2050P-IT, February 2021

Evaluation Concerns

By statute, SIPA is the official internet portal for the state of Colorado. However, SIPA is not subject to any administrative direction by any department, commission, board, or agency of the state. Accordingly, SIPA does not report to or take guidance and direction from the State's designated information technology leaders or officers. SIPA is not subject to the information security requirements and standards disseminated by these individuals and the organizations they represent. SIPA's existence predates statute to merge information technology service providers to a central state service.

Background

SIPA is responsible for developing and maintaining the officially recognized statewide internet portal. To meet this obligation, SIPA contracts with and oversees a statewide internet portal integrator (NIC Colorado) for the development, support, maintenance, and enhancement of state websites and web applications. This evaluation included a review of security of state websites and web applications developed and maintained by SIPA and its contractor.

Key Facts and Findings

- SIPA management has not established a strategy, program, or formalized processes for managing the security of systems and applications.
- SIPA's vendor management procedures and practices do not fully address the risks associated with information system security at their portal integrator.

Recommendations

- SIPA should establish policies and procedures to manage the security of people, processes, and technologies needed to develop and maintain state websites and web applications.
- SIPA should establish adequate vendor risk management practices to oversee the security activities of its portal integrator.

CHAPTER 1
OVERVIEW

Colorado Statewide Internet Portal Authority

The Colorado Statewide Internet Portal Authority (SIPA) is responsible for developing and maintaining the officially recognized statewide internet portal (Colorado.gov) that provides one-stop access to electronic information, products, and services in order to give members of the public, state agencies, and local governments an alternative way to transact business with the State. Statute requires SIPA to enter into a contract with and provide oversight of a statewide internet portal integrator for the development, support, maintenance, and enhancement of the equipment and systems utilized for the statewide internet portal [Section 24-37.7-105, C.R.S.]. SIPA has contracted with NIC Colorado (previously known as *Colorado Interactive*) to be its portal integrator. As the portal integrator, NIC Colorado maintains a team of project managers, software developers, database administrators, and other supporting staff. NIC Colorado also enters contracts with third- and fourth-party subservice providers to deliver products and services pursuant to its contract with SIPA. Accordingly, SIPA's role in the development and maintenance of the statewide internet portal is limited to oversight of NIC Colorado activities and contract deliverables.

Evaluation Purpose, Scope, and Methodology

The purpose of this evaluation was to determine whether state business conducted, or sensitive data transmitted, via state websites, applications and services developed and operated by SIPA are available and protected from unauthorized access and changes. Our evaluation also consisted of an assessment of the IT systems and security practices of NIC Colorado. See *Appendix A – Additional Scoping Information* for additional detail on the specific systems, websites, and web applications included in the scope of this assessment.

The scope of this evaluation consisted of two separate but coordinated assessments to identify and exploit application-level vulnerabilities that may exist due to configuration or coding errors. These assessments included (1) Web Application Security Assessment and (2) Security Processes and Controls Assessment. An overview of the objectives and scope for each of these phases and assessments is outlined in the paragraphs that follow.

The ***Web Application Security Assessment*** consisted of a series of technical tests to identify vulnerabilities in the implementation and configuration of SIPA systems. These tests included Vulnerability Assessment and Web Application Penetration Testing. To conduct these tests, a combination of proprietary tools and utilities, commercial products, and publicly available open-source tools were utilized. All testing was conducted from the Internet against infrastructure managed by NIC Colorado and its subcontractors.

- Vulnerability Assessment – We evaluated the security of over 130 state websites and web applications developed and/or maintained by SIPA and its portal integrator. A complete list of in-scope websites and web applications can be found in *Appendix A – Additional Scoping*

Information. The objective of this testing was to identify web application vulnerabilities that may exist due to configuration or coding errors. Utilizing configuration information provided by SIPA for key web-based applications, this testing mimicked attackers by exploring the applications and creating a list of potential application vulnerabilities. These potential vulnerabilities were then evaluated and verified.

- Penetration Testing – Utilizing the potential vulnerabilities identified through the vulnerability assessment, we identified a subset of twenty-four website and web applications determined to be of greater risk and attempted to exploit them as an attacker would. This exercise evaluated the realistic risk level associated with the successful exploitation of vulnerabilities, analyzed the possibility of attack chains, and accounted for any mitigating controls that may be in place.

The ***Security Processes and Controls Assessment*** consisted of an evaluation of the information security environment at SIPA and NIC Colorado in order to determine each organization's adherence to the State's information security policies or other leading industry standards or best practices for information security, in the following areas:

Access Management
Audit and Accountability
Configuration Management
Contingency Planning
Identification and Authentication
Incident Response
Personnel Security
Physical Security
Risk Assessment
Security Awareness Training
Security Planning
Software Development Life Cycle
System and Communication
System and Information Integrity

The testing methodology focused on areas of greatest risk to SIPA and state systems. Test procedures were designed and executed to determine if appropriate IT security controls were implemented, operating as intended, and producing the desired outcome with respect to meeting applicable security requirements, industry standards, or best practices.

Please Note: The detailed results of the web application security vulnerability assessment were provided to SIPA management under separate confidential cover. The results included detail on the specific problems and vulnerabilities we identified during the assessment as well as related information that SIPA can use to remediate them. Where applicable, within the findings of this report, we have included recommendations to assist SIPA with remediating any causes related to the problems noted during the security vulnerability assessment and penetration test.

CHAPTER 2

PUBLIC FINDINGS AND INFORMATION

SECURITY GOVERNANCE AND MANAGEMENT

A Board of Directors is the governing body of the Colorado Statewide Internet Portal Authority (SIPA) consisting of fifteen voting members with representation from both government and private sectors *(Section 24-37.7-102, C.R.S.)*. A majority of the Board is appointed by either the Governor or the Legislature, and as such, SIPA is considered a component unit by the State for financial reporting. As a political subdivision of the state, SIPA is not subject to any administrative direction by any department, commission, board, or agency of the state. Accordingly, SIPA does not report to or take guidance and direction from the State's designated information technology leaders or officers. SIPA is not subject to the information security requirements and standards disseminated by these individuals and the organizations they represent. For example, SIPA is not required to comply with the Colorado Information Security Policies (CISPs) and does not fall under the governance structures established by the Governor's Office of Information Technology (OIT).

In April 2020, the leadership of OIT and SIPA jointly signed a memo entitled *OIT and SIPA – Roles and Responsibilities*. This document formalized the partnership between OIT and SIPA, including key operating principles of each organization and their statutory basis for providing services to the state. In outlining the partnership, this document states, "SIPA complies with OIT standards…as applicable and appropriate." In addition, the document reiterates statute that, with regard to governance and oversight, SIPA "shall not be subject to administrative direction by any department, commission, board, or agency of the state."

The Chief Technology Officer (CTO) within SIPA is responsible for the management of the SIPA technology portfolio, strategic planning for new technology offerings, customer relationship management, compliance with technology standards and assisting the executive director with other business operations tasks. In this role, the CTO is SIPA's primary technical interface with its technology partners, including NIC Colorado. Except for the CTO, SIPA does not have additional staff or resources to oversee the cybersecurity activities of its technology partners.

Information security requirements for NIC Colorado related to the development, implementation, and management of State website and web applications are outlined in the *Colorado Statewide Internet Portal Authority Portal Integrator Contract with Colorado Interactive*, dated March 2014. This contract between SIPA and NIC Colorado states that the latter shall, "…adhere to Colorado Statewide IT Security Policies and Standards as required, for developed systems."

What was the purpose of our evaluation work and what work was performed?

The purpose of our work was to assess SIPA's cybersecurity governance practices, including policies and procedures, and planning and risk management processes to determine whether they were designed, in place, and operating effectively. To conduct our assessment and support our conclusions, we conducted interviews with members of the SIPA Board of Directors, SIPA leadership, and NIC Colorado personnel. We also examined and evaluated relevant statutes, contracts, and policy and procedure documents and inspected whether appropriate cybersecurity oversight and reporting mechanisms were in place over the related in-scope cybersecurity activities.

What problems did the evaluation work identify and how were the results of the evaluation work measured?

We identified the following problems at SIPA regarding cybersecurity governance and oversight:

1. SIPA management has not established a strategy, program, or formalized processes for assessing and managing risks associated with the security of information systems, including methods for determination of risk tolerance, risk mitigation, and risk acceptance.

   National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations – The first control (RA-1) under the Risk Assessment control family requires that the organization develops, documents, and disseminates a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

   NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations – The second step in the process of preparing a risk management framework is for the organization to establish a risk management strategy for the organization that includes a determination of risk tolerance.

   Control Objectives for Information and Related Technology (COBIT); Evaluate, Direct and Monitor (EDM) 03 – Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of information and technology is identified and managed. Information security risk is an integral part of enterprise risk and should be optimized within the enterprise risk appetite and tolerance.

   NIST Cybersecurity Framework v1.1, Risk Assessment (ID.RA) - The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

   The Government Accountability Office Standards for Internal Control in the Federal Government (The Green Book), Section 7.01. Management should identify, analyze, and respond to risks related to achieving the defined objectives. The following attributes contribute to the design, implementation, and operating effectiveness of this principle: Identification of Risks, Analysis of Risks, and Response to Risks.

2. SIPA management has not established policies and procedures for the management of information system security. Specifically, policies have not been established to address the security requirements and expectations for information technology systems developed, acquired, managed, and operated by SIPA and its partners. While the contract with NIC

Colorado does require adherence to Colorado Statewide IT Security Policies and Standards, these standards have not been adopted, tailored, or interpreted to address the needs of the relevant security environment and activities at NIC Colorado.

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations – The first control activity in each control family addresses the need for the organization to establish formal, document policies and procedures related to the specific control family (e.g., Access Control, Audit and Accountability, Configuration Management, etc.).

NIST Cybersecurity Framework v1.1, Governance ID.GV – The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

COBIT; Align, Plan and Organize (APO) 01.09 – Define and communicate policies and procedures. Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework.

The Green Book, Section 12.02-12.03. Management documents in policies the internal control responsibilities of the organization. Management documents in policies for each unit its responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness. Each unit, with guidance from management, determines the policies necessary to operate the process based on the objectives and related risks for the operational process. Each unit also documents policies in the appropriate level of detail to allow management to effectively monitor the control activity.

3. Roles and responsibilities are not clear in relation to State security policies. For example, it is not clear who the IT service provider is and who the business or data owner is of the State websites or web applications developed by SIPA. In addition, key security activities for account management and educating business and data owners were not being performed. Specifically, our testing of security control activities noted the following:
    - Agency user accounts are not disabled after ninety days of inactivity within State websites or custom web applications.
    - Security agreements are not in place for all Agency end-users of State websites. Our testing identified that for 7 out of a sample of 20 users, SIPA did not maintain a signed security agreement on file.

Colorado Information Security Policy (CISP) 001 through 018 – Section 8 of each policy document outlines key responsibilities for implementation of the policy, including those of the system's Business Owner. Section 7 of the CISPs define Business Owner as the agency or entity that owns the data, has the authority to authorize or deny access to the data, and is responsible for the accuracy, integrity, and timeliness of the data.

COBIT; APO 01.07 – Define information (data) and system ownership. Define and maintain responsibilities for ownership of information (data) and information systems.

CISP-001 Section 9.1.13 Account Management – IT Service Provider shall configure Information Systems to automatically disable or make inactive accounts after 90 days of inactivity.

The Green Book, Section 10.02. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives.

4. SIPA has not formally established expectations or defined the staff skills and experience required to address objectives and risks in relation to established information security policies or best practices.

   COBIT APO 01.08 – Define target skills and competencies. Define the required skills and competencies to achieve relevant management objectives.

   COBIT APO 07.03 – Maintain the skills and competencies of personnel. Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.

   The Green Book, Section 4.02. Management establishes expectations of competence for key roles, and other roles at management's discretion, to help the entity achieve its objectives. Competence is the qualification to carry out assigned responsibilities. It requires relevant knowledge, skills, and abilities, which are gained largely from professional experience, training, and certifications. It is demonstrated by the behavior of individuals as they carry out their responsibilities.

   The Green Book, Section 4.04. Personnel need to possess and maintain a level of competence that allows them to accomplish their assigned responsibilities, as well as understand the importance of effective internal control. Holding individuals accountable to established policies by evaluating personnel's competence is integral to attracting, developing, and retaining individuals. Management evaluates competence of personnel across the entity in relation to established policies. Management acts as necessary to address any deviations from the established policies. The oversight body evaluates the competence of management as well as the competence overall of entity personnel.

Why did the problems occur?

SIPA stated that, as a technology procurement and management organization, it has not identified the need for an information security risk management program. SIPA has managed risk related to the security of IT services through contract requirements and regular project and management meetings. Additionally, SIPA relies on its close partnerships with NIC Colorado and OIT security staff when questions related to security risk arise.

Why do these problems matter?

Governance is the foundation of cybersecurity at any organization. It is for this reason that Colorado Statutes, applicable to the Governor's Office of Information Technology, require the appointment of both a Chief Information Officer and Chief Information Security Officer to oversee information security for the State of Colorado. These individuals establish security strategies, policies, procedures, expectations and standards for the organization and its business partners. They are responsible for evaluating risk, making decisions, and ensuring consistency in the implementation of security. Hiring staff who have adequate security experience is important to function adequately in these roles; however, if they leave the organization, their replacements may not have the same level of knowledge and experience with standards or expectations for cybersecurity. Similarly, engaging with a competent and reliable contractor is important; however, personnel changes or unforeseen pressures may negatively impact the cybersecurity control environment. Not addressing the governance and management issues identified in the finding may have the following impacts:

- Security measures and investments made by SIPA and its partners may not adequately address the security risks faced by the organization.
- Security expectations for SIPA personnel, partners, and customers may be unclear.
- Security roles and responsibilities may be unclear or may not be communicated to or understood by those responsible.
- Security reports provided by NIC Colorado may not be adequately scrutinized or evaluated. Potential security shortcomings or vulnerabilities may not be addressed.

Recommendation 1:

The Colorado Statewide Internet Portal Authority (SIPA) should improve security governance and management processes and controls by:

1. Establishing, with input from the Board, policies and procedures for managing risks related to information security. SIPA should seek input from the Board and establish requirements for conducting periodic security risk assessments, based upon an industry-recognized security framework, and utilizing the results of these assessments to determine areas of risk tolerance, risk mitigation, and risk avoidance. In addition, these policies and procedures should also establish requirements for periodic reporting of the status of security risk to the Board.

2. Developing formal policies and procedures for the management of information security. These policies and procedures should cover, but not be limited to, the relevant aspects of security necessary to ensure the confidentiality, integrity, and availability of systems and services provided by SIPA to the State, address the security roles and responsibilities of SIPA personnel, partners, and data owners (e.g., State agencies or offices), define a frequency by which these policies and procedures will be reviewed and approved by SIPA management, conducting a review and approval in line with the determined frequency.

3. Developing and clarifying in policies and procedures expected roles and responsibilities as they relate to state Security Policies. These policies and procedures should include expectations for account management and for providing timely and periodic training to these individuals on their security roles and responsibilities.

4. Conducting an evaluation of the skills and competencies of the SIPA staff to identify gaps in the organization's security knowledge and experience with developing and executing a plan for addressing those gaps.

Colorado Statewide Internet Portal Authority Responses:

1. **Agree. Implementation Date: December 2021.** SIPA will work with the Governor's Office of Information Technology and a third-party vendor partner and the Board to develop a policy and procedure for managing information security risk that includes, but is not limited to, conducting periodic security risk assessments, based upon an industry-recognized security framework, and utilizing the results of these assessments to determine areas of risk tolerance, risk mitigation, and risk avoidance. This policy will also outline periodic reporting of the status of information security risk to the Board.

2. **Partially Agree. Implementation Date: December 2021.** SIPA partially agrees with this recommendation. SIPA does not have the statutory authority to compel data owners (e.g., State agencies or offices) to comply with a policy developed by SIPA. SIPA will work with the Governor's Office of Information Technology and a third-party vendor partner to analyze the Statewide Information Security Policies as they related to the systems that are operated by its vendor in order to develop a policy and procedure for the management of information security, to ensure the confidentiality, integrity, and availability of systems and services provided to the State and local governments. This policy will address the security roles and responsibilities of SIPA personnel. The policy will be reviewed and approved annually by SIPA management.

   AUDITORS ADDENDUM: Like most IT service providers, SIPA should establish expectations for the users of the systems and services it provides. The establishment of formal policies and procedures, including roles and responsibilities addressing data owners, does not necessarily require SIPA to enforcement those policies. A policy could simply establish precedent or expectation. SIPA should continue to work with all parties involved in the ongoing support and management of systems it develops for the State to ensure control activities intended to address security risks are conducted, or at minimum understood.

3. **Agree. Implementation Date: December 2021.** SIPA will ensure that the requirement for the definition of roles and responsibilities related to State Security Policies and expectations around account management and periodic training are outlined in the policy developed as a result of Recommendation 1, Part 2 of the Security Governance and Management Recommendations finding.

4. **Agree. Implementation Date: December 2021.** SIPA implemented annual cybersecurity training in 2019 for all staff. While SIPA believes that its staff is addressing security governance and management, SIPA will work with the Governor's Office of Information Technology and a third-party vendor to assess the skills and competencies related to security and develop a plan for addressing any gaps that are discovered.

GLOSSARY

Access Controls

Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.

COBIT

COBIT (Control Objectives for Information and Related Technologies) is a framework created by ISACA for information technology (IT) management and IT governance. The framework defines a set of generic processes for the management of IT, with each process defined together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementary maturity model

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policies

Information Security Policies are a definition of what it means to be secure for a system, organization or other entity

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

NIST SP 800-53 Revision 4

NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce.

Penetration Testing

A penetration test, colloquially known as a pen test, or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

System

For the purpose of this evaluation, a “system” is the collective sum of an electronic computer application, as well as its accompanying operating system and database.

The Green Book

Standards for Internal Control in the Federal Government, known as the "Green Book," sets the standards for an effective internal control system for federal agencies.

Vendor Risk Management

Vendor risk management is defined as the process of ensuring the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Web Application

A web application is application software that runs on a web server, unlike computer-based software programs that are run locally on the operating system of the device. Web applications are accessed by the user through a web browser with an active internet connection

APPENDIX A – ADDITIONAL SCOPING INFORMATION

The following is a listing of state websites and web applications developed or hosted by SIPA that were included within the scope of our Web Application Penetration Testing.

- Agriculture Cashier Payment Portal
- App Engine Onboarding Questionnaire
- Board of Assessment Appeals Online Filing
- Broadband Fund
- CAPS Check Unit
- CDA Commercial Pesticide Applicator License Backup
- CDA-Conservation Services Division- Request A Bug
- CDHS Boards and Commissions
- CDLE Customer Support Requests
- CDLE Penalty Orders
- CDLE Self Insured Filings Data Submission
- CDLE Self Insured Filings Payments
- CI Office Guest Registration
- CI Test App
- CMS Project Questionnaire
- Cold Case
- Colorado Aging Strategy
- Colorado Behavioral Health Ombudsman
- Colorado Bureau of Investigation
- Colorado Business Emergency Operations Center
- Colorado Cancer Plan
- Colorado Commission on Affordable Health Care
- Colorado Decision Support Systems
- Colorado Department of Agriculture
- Colorado Department of Health Care Policy and Financing
- Colorado Department of Human Services
- Colorado Department of Labor and Employment
- Colorado Department of Local Affairs
- Colorado Department of Personnel and Administration
- Colorado Department of Public Health and Environment
- Colorado Department of Public Safety
- Colorado Department of Regulatory Agencies
- Colorado Department of Revenue
- Colorado Department of the Treasury
- Colorado Division of Reclamation, Mining and Safety
- Colorado Division of Veteran's Affairs
- Colorado Environment Public Health Tracking Program
- Colorado Environmental Public Health Tracking
- Colorado Health Professional Check
- Colorado Local Public Health and Environment Resources

- Colorado Marihuana - Spanish
- Colorado Marijuana - English
- Colorado Mitigation and Recovery Site
- Colorado Parks and Wildlife Donations ONL
- Colorado Public Utilities Commission
- Colorado Rural Workforce Consortium
- Colorado State Archives
- Colorado State Capitol
- Colorado State Land Board
- Colorado State Land Board - Invoice Payments
- Colorado State Patrol
- Colorado Water Conservation Board
- Colorado Water Plan
- Colorado Workforce Development Council
- Colorado.Gov Feedback
- Commission on Criminal and Juvenile Justice
- Contact Compass
- Courts Payment and Billing
- COVID-19
- Department of Agriculture - Brand Book Order Form
- Department of Agriculture - Farm Fresh Directory Listing
- Department of Agriculture - Private Pesticide Applicator Exam Materials Request
- Department of Agriculture - Private Pesticide Applicator License
- Department of Higher Education
- Department of Military and Veterans Affairs
- Department of the Treasury - Scheduling Request
- Disability Determination Services
- Disability Funding Committee
- Division of Animal Health
- Division of Brand Inspection
- Division of Capital Assets
- Division of Central Services
- Division of Conservation Services
- Division of Criminal Justice
- Division of Fire Prevention and Control
- Division of Homeland Security and Emergency Management
- Division of Human Resources
- Division of Inspection and Consumer Services
- Division of Laboratory Services
- Division of Markets
- Division of Motor Vehicles
- Division of Oil and Public Safety
- Division of Plant Industry
- Division of Professions and Occupations
- Division of Vocational Rehabilitation

- DOR OTC Tax Payments
- DORA eLicensing Reports
- DPA State Archives Online Payment
- Driver Monitoring
- Driver Records - Interactive
- Driver Records - Point to Point
- DRIVES - Portal Detail File
- DRMS Coal Mine Official Certification
- Enforcement Division
- Enterprise Zone Pre-Certification- Certification
- Feedback Utility
- Gambling Intercept Payment
- Gov2Go CO Flag Status Notification
- Governor's Residence Event Scheduling Request
- Governor's Residence Event Scheduling Request
- Governor's Summer Job Hunt
- Health Care Policy and Financing Community Mapping & Reporting
- HR Works
- Integrated Criminal Justice Information System
- John's Test App
- Liquor Enforcement - Event Application
- Long-Term Care Partnership
- Military and Veterans Programs
- Minors in Possession (MIP)
- Monitoring Health Concerns Related to Marijuana
- Monitoring Health Concerns Related to Marijuana
- Motor Vehicle Verification System
- Motorists Insurance Information Database- MIIDB
- MyBizColorado
- Office of Administrative Courts
- Office of Policy, Research, and Regulatory Reform
- Office of Research and Statistics - DCJ
- Office of the State Architect
- Office of the State Controller
- OIT Transparency Application
- Online Surcharge Filing
- Payment Engine/CORE Integration
- Prescription Drug Monitoring Program
- Private Pesticide Applicator License Renewal
- Public Employees' Social Security Program
- RAS and ACH File Service
- School Safety Resource Center
- Sex Offender Registry and Mapping
- State Employee Assistance Program
- State Land Board

- State Personnel Board
- State Telephone Directory
- Storage Tank Online Payment System
- Take 5 to Get Wise
- Taxation Division
- Youthful Driver Monitoring