Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

Memorandum

Room 029 State Capitol, Denver, CO 80203-1784
Phone: (303) 866-3521 • Fax: (303) 866-3855
lcs.ga@coleg.gov • leg.colorado.gov/lcs

February 13, 2023

TO: Joint Technology Committee

FROM: Vanessa Reilly, Senior Research Analyst, 303-866-4753
Joint Technology Committee Staff

SUBJECT: JTC Staff Analysis of Executive Committee-Referred FY 2023-24 Legislative Information Services Budget Request

Summary of Request

Legislative Information Services (LIS), the General Assembly's information technology (IT) section (housed in Legislative Council Staff), requests an increase for FY 2023-24 of $261,000 General Fund in one-time funds, and $461,180 General Fund and 4.0 FTE ongoing. The Executive Committee referred this request to the Joint Technology Committee (JTC) for the committee's review and recommendation.

Table 1 outlines the costs and FTE associated with each portion of the request. The project costs are described in further detail below.

Table 1
Request Detail

Request	One-time	Ongoing	FTE
Accessibility Compliance	$261,000	$100,000	1.0
Subscription Service Licenses		$21,180	0.0
Cybersecurity and Application Development Staff		$340,000	3.0
Total		$461,180	4.0

***Open records requirements**: Pursuant to Section 24-72-202 (6.5)(b), C.R.S., research memoranda and other final products of Legislative Council Staff are considered public records and subject to public inspection unless: a) the research is related to proposed or pending legislation; and b) the legislator requesting the research specifically asks that the research be permanently considered "work product" and not subject to public inspection. If you would like to designate this memorandum to be permanently considered "work product" not subject to public inspection, or if you think additional research is required and this is not a final product, please contact the Legislative Council Librarian at (303) 866-4011 within seven days of the date of the memorandum.*

Accessibility Compliance

One-time funds for accessibility audit. The request seeks $261,000 in one-time funds to contract with a vendor to perform accessibility audits of a representative portion of the General Assembly's website, publications, and applications. Automated accessibility scanning tools have identified 60,000 web pages and 74,000 PDFs that will likely require remediation; in addition, the agency has identified more than 50 internal and public-facing applications that require audit and remediation. Because automated tools are only able to identify roughly 30 percent of accessibility issues, an audit is needed to identify the scope of accessibility deficiencies in the General Assembly's digital assets. As the first step towards compliance with House Bill 21-1110, the audit will provide the General Assembly with necessary information to identify resources that will be needed in the future to remediate identified deficiencies. LIS anticipates submitting additional accessibility-related budget requests in the future to remediate issues identified by the audit.

According to the agency, the audit will be performed on a representative portion of the General Assembly's website, publications, and applications. The one-time funds requested for the audit are based on an estimate received from Level Access, an accessibility vendor included in the Office of Information Technology's list of Approved Vendors for Accessibility Testing. The agency sought estimates from five vendors total; only Level Access provided an estimate based on the entire scope described in LIS' Accessibility Audit Outline. Additional information on vendor selection can be found in the agency's responses to staff questions, included as Attachment A.

Lead Accessibility Analyst. The request also seeks $100,000 base salary ongoing for 1.0 FTE for a Lead Accessibility Analyst, to lead the General Assembly's accessibility compliance efforts. Among other duties, the FTE will be responsible for implementing the General Assembly's accessibility plan, incorporating accessibility into the procurement process, working with the LIS application development team to create processes that ensure new content is accessible from the point of creation, and creating testing standards to confirm ongoing compliance. The Lead Accessibility Analyst will also be responsible for managing the accessibility audit. According to the agency, without this new FTE, existing LIS staff will be reallocated from other projects to lead compliance efforts, which will reduce and delay delivery of LIS services to the General Assembly.

Program Information. *House Bill 21-1110*, *Colorado Laws for Persons with Disabilities*, strengthened state discrimination laws for individuals with disabilities. The bill, which requires state agencies to fully implement accessibility plans by July 1, 2024, also added three discrimination violations and provided additional responsibility for OIT to improve the accessibility of state agency web content. The bill prohibits:

- the exclusion of an individual with a disability from participation in or the benefits of services, programs, or activities provided by a public entity;
- a state agency from promulgating rules that provide less protection for individuals with disabilities than provided by the ADA; and
- a public entity from failing to comply with accessibility standards established by OIT.

Because the bill expands the definition of "public entity" under Colorado civil rights law to include "any department, agency, special district, or other instrumentality of a state or local government", the bill's provisions extend to the General Assembly.

Subscription Service Licenses

Zoom Licenses. The request seeks $14,400 ongoing to provide up to 80 additional Zoom licenses for legislative staff. Zoom licenses are provided at a cost of $180 per license per year. Demand for tools that support the hybrid work environment continues to be strong both internally, as well as when legislative employees interact with outside stakeholders and executive branch employees. New licenses will be allocated as follows in Table 2.

Table 2
Allocation of New Zoom Licenses

Agency	Number of Licenses
Office of the State Auditor	25
Office of Legislative Legal Services	32
Legislative Council Staff	10
Other Partisan & Nonpartisan Staff	13
Total	80

Legislative service agencies currently use Zoom for internal meetings, as many staff continue to work remotely, but also to meet with auditees, legislators, lobbyists, stakeholders, NCSL workgroups, and to interview new hire candidates. According to LIS, the most significant current need comes from the Office of the State Auditor (OSA) and the Office of Legislative Legal Services (OLLS). OSA primarily interacts with executive branch departments in their audits; Zoom is the primary means of conducting meetings as many of these employees are now working remotely. OLLS would prefer every member of staff have their own Zoom account; or, in lieu of that request, that at least every attorney have an account.

Box Licenses. The request seeks $6,780 ongoing to provide up to 30 additional Box licenses for legislative staff. Box licenses are available at a cost of $226 per license per year. Box allows for secure, cloud-based file storage that enables easy collaboration and access to shared documents. Of the requested additional licenses, 11 will be allocated to OSA; the remaining 19 will be available for other partisan and nonpartisan staff. According to LIS, OSA uses Box accounts to store, transfer, and share data between auditors and auditees. Much of this data is subject to statutory confidentiality requirements and is located in files that are typically too large to email, making Box's platform essential to maintaining audit security.

Cybersecurity and Application Development Staff

The request seeks $340,000 ongoing as base salary for 3.0 FTE for the following new staff:

- Application Cybersecurity Analyst / Java Developer: $125,000 and 1.0 FTE;
- Business Analyst / Quality Assurance Analyst: $90,000 and 1.0 FTE; and
- Ruby on Rails Developer / DevOps Engineer: $125,000 and 1.0 FTE.

Application Cybersecurity Analyst / Java Developer. The Application Cybersecurity Analyst / Java Developer role will focus primarily on application security. The General Assembly utilizes several custom internal and public-facing applications that must be kept secure to ensure availability, prevent attacks, and protect sensitive information. The role will be responsible for implementing security controls to identify and patch vulnerabilities, setting security design requirements during the software creation and development stage, and will have familiarity with web application vulnerabilities and remediation techniques. According to LIS, including a developer who is focused on security on the team will improve integration of application security into development processes. Java development is secondary to the cybersecurity duties, and will primarily be relied upon during urgent stakeholder request surges.

Business Analyst / Quality Assurance Analyst. The Business Analyst / Quality Assurance Analyst FTE will work closely with customers to understand, identify, and document business needs in advance of development projects, and will then test applications created by LIS developers to ensure they meet customer needs. According to LIS, combining these roles supports better understanding of business processes and needs, which improves product quality and developer productivity. Having experienced recent turnover in long-tenured staff and anticipating other impending retirements, the agency also believes that combining these roles allows for better maintenance of institutional knowledge. Currently, lack of business analyst availability has created bottlenecks in LIS' development processes, leading to inefficient use of resources and project delays.

Ruby on Rails Developer / DevOps Engineer. The Ruby on Rails Developer / DevOps Engineer role will focus primarily on working with all platforms to develop the agency's DevOps strategy. LIS is currently performing DevOps differently across all platforms, which results in inefficient use of resources and sometimes require work be redone. The new FTE will work with each platform's development team to plan and implement a secure and uniform strategy. Ruby on Rails development will be secondary to DevOps change management duties and will primarily be relied upon during urgent stakeholder request surges.

Program Information. The LIS application development team includes staff who perform development, business analysis, quality assurance, user interface design, create technical architecture, and project management. The team supports a number of legacy and newly-developed applications that provide a technical foundation for the legislative process. Thanks to the high application to developer ratio, LIS employs interrupt-driven development which requires developers to balance project work with responding to stakeholders as needed. According to the agency, in order to balance these various needs with the need to make budget requests that are as conservative as possible, several types of roles are often combined into a single FTE.

Attachment A

FY 2023-24 General Fund Information Technology Budget Request

Colorado Legislative Council Staff (LCS)
Legislative Information Services (LIS)

Joint Technology Committee Staff Questions

Please respond by end of day February 9, 2023
to: jtc.ga@coleg.gov

Accessibility requests

1. Please describe the basis for how the $261,000 vendor cost was estimated. The submission memo explains that the estimate was based on a sample data set provided to five vendors, but that the $261,000 represents the estimate from a single vendor, Level Access. What were the other vendors' cost estimates?

LIS asked vendors to respond to an "Accessibility Audit Outline," which is described in more detail below. As part of the outline, LIS asked vendors to provide estimates for auditing a small subset of content, which consisted of five unique web pages and six unique PDF files, in order to understand each vendor's pricing model. We received three kinds of estimates:

1) only Level Access provided an estimate based on the entire scope described in Accessibility Audit Outline;
2) estimates from four vendors, including Level Access, for auditing the smaller subset of content that included five unique web pages and six unique PDF files; and
3) an estimate from the Blind Institute of Technology that didn't use either the outline or the smaller subset, but was based on 2,500 unique documents/web pages.

Each of these is described below.

Level Access estimate on the entire scope of the Accessibility Audit Outline. The $261,000 estimate from Level Access is based on the "Accessibility Audit Outline," which covers a broad range of unique document types and applications that are a representative sample of the digital content produced by the General Assembly's staff and systems. The outline also included an overview of the type of work that would be done during an accessibility audit and references the accessibility requirements adopted by OIT. It also provided the vendors with insight into how the vendors will be evaluated and touches on the required qualifications and experience expected by the branch.

We requested this amount because it represents a more realistic estimate on the actual scope of auditing required to meet the requirements of House Bill 21-1110 in FY 2023-24.

Subset of 5 web pages and 6 PDFS. The following vendors provided cost estimates on a much smaller subset of content than what was included in the Accessibility Audit Outline, which included five unique web pages and six unique PDF files. This subset of content is much smaller than the broader sample detailed in the Accessibility Audit Outline:

a. Crownpeak + iLUMINO: $9,000
b. Level Access: $20,090. This estimate is contained within the $261,000 estimate that Level Access provided for the broader sample in the Accessibility Audit Outline.
c. Online ADA: $1,828 for five web pages; $19,800 for six PDFs. Total: $21,628
d. TPGi: $9,680 for five web pages; $2,635 for six PDFs. Total: $12,315

The Blind Institute of Technology provided a $97,000 estimate to audit 2,500 unique documents/web pages.

2. The submission memo explains that Level Access is an accessibility vendor with which OIT has previously contracted. However, OIT's accessibility budget request uses an estimate from Siteimprove, not Level Access. What services and products does Level Access provide compared to other estimates received?

The OIT references Level Access among their Approved Vendors for Accessibility Testing Services on the following page:
https://docs.google.com/spreadsheets/d/1e_kEJL2uYyWO4GSqbJZHJyKuJUEUGpvLquMOIoe01s0/edit#gid=0

We consulted Gartner about accessibility vendors, which they classify as either "full-service providers" or "technology-first providers." They classified Level Access and TPGi as "full-service providers" and Crownpeak + iLUMINO as a technology-first provider. They summarized the services from these types of providers as follows:

1) Full Service Providers (Level Access and TPGi) provide the following services:

a. scanning tools to automatically identify accessibility issues and automatically remediate issues, where possible;
b. platforms for auditing, monitoring and accessibility engineering (developer tools);
c. options for "human in the loop" issue identification (to ensure all issues are known);
d. training on their platform, as well as general accessibility training;
e. full custom consulting services; and
f. full legal support services.

2) Technology First Providers (Crownpeak + iLUMINO) provide the following services:

a. scanning tools to automatically identify accessibility issues and automatically remediate issues, where possible;
b. platforms for auditing, monitoring and accessibility engineering (developer tools);

c. options for "human in the loop" issue identification (to ensure all issues are known);
d. training on their platform, as well as general accessibility training;
e. limited (or "canned") consulting services, such as auditing and certification services; and
f. limited (or "canned") legal support services.

The Blind Institute of Technology and Online ADA vendors were not classified by Gartner, but provide the following services:

1. Testing, auditing and evaluation services;
2. reporting services;
3. written compliance plan development;
4. compliance plan implementation services; and
5. Online ADA also provides project management services, but the Blind Institute of Technology does not.

3. Is there a current estimate for the number of accessibility deficiencies that LIS expects to need to address? What is the approximate number of webpages and applications that will require future remediation? How have policies changed since the passage of House Bill 21-1110 to ensure that new deficiencies are not being created and implemented prior to this budget request?

Estimated number of deficiencies. The number of deficiencies is unknown at this time and is the primary purpose of requesting funds for an audit and FTE. The audit will reveal the deficiencies on a representative sample of the digital content produced by General Assembly's staff and systems. The requested (Lead Accessibility Analyst) FTE will use their expertise to help ensure the General Assembly gets the most from the audit.

Most of the 60,000 web pages and 74,000 PDFs identified by Siteimprove (an accessibility scanning tool) may require remediation. A core function of the audit will be to manually identify what Siteimprove does not catch. Siteimprove's auditing tool will typically identify 30% of accessibility issues.

More than 50 internal and public facing applications have been identified as requiring auditing and remediation. Prominent applications include:

1) The General Assembly's Website;
2) Live Proceedings;
3) iLegislate;
4) the LCS Research Request application;
5) the Voting System;
6) the XDOME CRS Publishing application;
7) CLICS (Including bill drafting, committee management, document management, work flow, and publish applications); and
8) The Visitor Services Tour System.

Please note that we plan to prioritize newly created and the most accessed content ahead of archived digital content for remediation.

Policy changes since House Bill 21-1110. Policy updates and changes are a part of the General Assembly's IT accessibility roadmap. Incorporating accessibility into digital services and projects is an ongoing process and not a one-time effort. We will continue to build accessibility processes and procedures in the development of our digital content.

4. Does LIS expect to request additional long-term FTE in out-years to address remediation needs, or is remediation work anticipated to be performed on a contract basis? Can LIS integrate accessibility into existing processes and procedures, thus eliminating the need for a full FTE in future? Please explain the need to fund a full-time Lead Accessibility Analyst before the first accessibility audit provides its findings.

Both additional long-term FTE and contract services will likely be needed in out-years. Additional FTE may be needed for in-house remediation efforts. Contract services may be used for on-demand document remediation and expert consulting. The accessibility audit will provide information essential to understanding the resources needed to achieve compliance.

LIS does not currently have the capacity to integrate accessibility into existing processes and procedures. **An FTE with expertise in accessibility will be essential to ensure that accessibility is incorporated into all processes and content by:**

- further developing, maintaining, and implementing the accessibility plan;
- managing the accessibility vendor audit, remediation, and consulting work;
- serving as an expert on the accessibility standards set by OIT, and assistant all staff in the legislative branch with meeting these standards;
- performing compliance officer duties for new and existing digital content;
- incorporating accessibility in the procurement process with vendor management, product evaluation, and oversight;
- working with the application development team to create requirements needed to achieve compliance; and
- creating testing standards to ensure that compliance requirements are met.

5. What are the possible consequences if an accessibility audit and/or Lead Accessibility Analyst is not funded? What alternative options were considered?

The consequences of not performing an accessibility audit include the following:

- the accessibility deficiencies of the General Assembly's documents, web pages, and applications would remain an unknown;

- the resources needed to achieve compliance with House Bill 21-1110 would remain unknown; and
- the scope of deficiencies on the General Assembly's website will remain unknown. Siteimprove's auditing tool will typically identify 30% of accessibility issues for web pages. Manual testing, a core component of the audit, is needed for the remainder of issues and non-web based applications.

The consequences of not funding a Lead Accessibility Analyst include the following:

- existing LIS staff would need to be reallocated from other projects to lead the compliance effort, which would mean reduced services to the legislative branch elsewhere;
- LIS would lack the expertise to oversee accessibility plan development, implementation, compliance oversite, and accessibility vendor management; and
- the compliance effort and existing application development efforts would be significantly impacted and progress at a slower rate.

Operating requests

6. The request adds 80 Zoom accounts.
   a. Please summarize the existing Zoom license agreement.

      Enterprise Named Host
      Large Meeting 500 participants
      Webinar 500 participants
      Quantity: 201
      Subscription period: May 27, 2022 - May 27, 2023 (Annual)

   b. How many Zoom accounts do the respective offices currently have, compared to the number of staff per office?

      Online meetings continue to be a popular and productive manner of meeting, even as the pandemic is winding down. And with so many people working in a hybrid work model, online meetings have become the de-facto standard in recent years.

      Since each office's roles and responsibilities differ, so also does each office's needs for Zoom accounts. Staff of the Office of the State Auditor primarily interact with executive branch departments for performance, financial and IT audits. Since a lot of auditees have moved to working from home, Zoom has become the primary means of conducting meetings. This has resulted in a much greater need for the OSA.

      Similarly, OLLS, uses Zoom for meetings with members, lobbyists, stakeholders, NCSL workgroups, internal office team/workgroup meetings, and interviews of prospective new hires. If the budget allows, OLLS would prefer every person to have their own Zoom account. If this is not possible, they are requesting that every attorney have a Zoom account.

While not all legislators currently have an enterprise Zoom account, the intent is to have the capacity to provide every legislator with an enterprise Zoom account if they so desire.

Table 1. Existing Legislative Branch Zoom Accounts

Groups	Count
Committees	47
House	2
JBC	2
LCS	11
LIS	25
OLLS/OLWR	6
OSA	38
Senate	2
Senators	2
Representatives	2

c. Does LIS have data to show how frequently the existing accounts are used?
Yes.

d. Are accounts only available on an annual basis, or could monthly licenses be purchased during session/busy periods to supplement existing licenses?

We have asked Zoom about this possibility and for pricing options for some licenses to be used for a partial year. However, we are still waiting to hear back from someone at Zoom; our usual Zoom account representative has been impacted by layoffs.

While most business functions would require the use of Zoom throughout the year, there are some licenses that tend to be used primarily during the session. Sometimes, these accounts are repurposed for other functions. For example, some committee accounts may also be used for staff blue book meetings. Having said that, limiting and repurposing these accounts in this way does add account management overhead and potential user inconvenience, resulting in customer satisfaction issues for only limited realized savings.

7. Will the remaining 13 Zoom licenses and 18 Box licenses be allocated to particular partisan and nonpartisan staff? If not, how will they be apportioned amongst staff?

To be clear, this appropriation gives us the flexibility to add additional licenses if required. Additional licenses will be purchased only if needed. The remaining Zoom and Box licenses will be provisioned based on the business need in the legislative institution and is not apportioned by specific agency, partisan or non-partisan staff. The existing available Zoom licenses will first be provisioned to the required staff as mentioned above and in the budget request, and the additional funded licenses will be procured as needed for members to use for legislative work.

8. Please confirm that LIS is requesting $14,400 for Zoom licenses and not the $18,000 noted in the "Description" column of Table 2: Operating Budget Requests. Did LIS consider asking for more Zoom licenses initially, and if so, why?

   LIS initially considered a larger request. The need expressed by legislative staff agencies was much broader than the amount requested. LIS rationalized the requests to balance an appropriate request with the business needs. The spare licenses are also requested to factor in potential needs in the future and to ensure there is no disruption caused to the business of the legislature.

9. What are the possible consequences if Zoom licenses are not funded?

   Staff will have to continue using either personal paid licenses or free licenses with limited functionality to do their work for the legislature. When meeting with non-legislative meeting participants, legislative staff may need to depend on other participants to initiate the Zoom meeting. If there is a need for more licenses for committees or other needs that need to be fulfilled, we would repurpose licenses from existing users. Staff will continue to adapt to the best of their abilities.

10. The submission memo explains that the Box funding request is to "expand the offering to most staff so that they can use Box functionality for collaborating with members and other staff."

    a. How does LIS monitor usage of Box to ensure that each license is being used?

       LIS monitors usage of Box usage on an ad-hoc basis. LIS is not requiring accounts to be deleted if no activity is detected. LIS is taking the approach of reaching out, encouraging and training account owners on use of their Box accounts. Every member gets a Box account, irrespective of usage. These Box accounts are integrated with other applications, such as iLegislate and CLICS.

    b. Please provide statistics describing the current usage of Box among members and staff. What is the percentage of staff that use free accounts?

       Accounts not created within the *coleg* enterprise instance are outside the purview of our oversight. As a result, we do not have accurate knowledge of free accounts created and managed outside of the enterprise instance.

    c. What are the other content management and collaboration tools used among members and staff?

       Other than using the iLegislate app to share custom bill content with members, email is the only other content management and collaboration tool used between members and staff.

    d. What are the possible consequences if additional Box licenses are not funded? What alternative options were considered?

The additional Box licenses are for the OSA's individual contributor auditors. OSA uses Box licenses to store, transfer and share data content between auditees and the auditors. Box is a preferred tool for auditors because much of the data they must share are subject to statutory confidentiality requirements and are shared in very large files that may not be easily emailed. Without the additional Box licenses, they will continue using less secure alternate methods.

11. The submission memo explains that the Box funding request will add an "additional 30 users at an annual cost of $226 per enterprise account." Does the license agreement limit the amount of storage? If Box licenses include a storage limit, please describe the department's data retention policy, including purging and archiving obsolete or outdated data.

    The legislature's Box enterprise instance allows for unlimited data storage.

12. Please summarize the data confidentiality requirements and controls in place to secure the data stored in Box. Please also include a summary of the license agreement with Box to secure the Colorado General Assembly (CGA) data, including the contractual responsibility of each party.

    As of 2019, each file uploaded to Box is encrypted with a unique key and that key is then encrypted with a Key Encrypting Key (KEK). Content uploaded to the Box service is encrypted in transit using transport layer security (TLS). Box supports AES 256-bit encryption.

    Box enforces the logical segmentation of customer (tenant) data through business logic controls, combined with encryption of each uploaded file with a unique key.

    When users log in to Box the very first time, they are presented with terms and conditions depending on if they are internal or external users. In general, licensed users are asked to use it only for official state business, protect their password, and do no harm. The released and reviewed terms and conditions document is available on request.

New full-time employee (FTE) requests

13. Table 3 states that a Business Analyst/Quality Assurance Analyst (BA/QA) will "improve cross-training and reduce the loss of institutional knowledge resulting from attrition."

    a. Regarding the BA/QA position in the request, please describe the project methodology LIS uses, and the need to combine the business analyst and quality assurance roles. If LIS uses an agile methodology, please also explain the traditional role of a product owner compared to the BA/QA position in the request.

       LIS employs an interrupt-driven development methodology. This is a direct result of the high application to developer ratio that exists at the Colorado General Assembly. Developers must perform project work in parallel with providing stakeholder support. In order to fulfill surges in specific internal and external stakeholder needs, we need resources that can perform different roles. We currently have developers and project managers also filling business analyst and quality assurance roles for certain projects due to stakeholder demand. Due to the large number of applications, LIS has in the past, depended on resources within some of the staff agencies to fill the Product Owner role that should reside within LIS. Turnover in these staff agencies have resulted in brain drain that, in turn, has had a major impact on the user experience for these applications.

b. Please provide more information describing the plan for cross-training, including existing BA/QA staff, and the risk of losing institutional knowledge.

With increasing digitalizing of the legislature's business, the technology footprint within business capabilities is growing. Applications range from general business functions (such as leave management) to specific business functions (such as audit submissions, research requests, budget management, bill drafting, statutes publishing, etc.). LIS has a small team of business knowledge experts. As such, it is imperative that LIS staff understand multiple business processes intimately and how they translate into applications.

The risk of losing institutional knowledge will never be zero, but LIS is working to minimize that risk. All new BA/QA staff are assigned a Product Owner role in at least one new project and at least one existing legacy product. They also perform QA duties for at least one other project. They work closely with at least one senior BA, QA, and IT Manager in all of their projects to ensure they are following LIS guidelines. To minimize the impact of losing institutional knowledge, LIS has assigned primary and secondary Business Analysts and Developers for all applications. Because it is easier to develop BA and QA skills than to learn the legislative business, LIS focuses on hiring resources with core knowledge of the business and trains them on BA and QA skills.

14. Please provide more information about the request for a Java developer who will also implement new application security controls, processes, procedures, and tools.

a. What is the Java experience needed for this position, including the number of years coding custom applications? What is the application security experience needed for this position, including the number of years driving and managing application security changes, and monitoring new security controls?

The primary duty for this role is application security, and Java development is secondary. We are looking for someone with 3-5 years of Java development in case development help is needed during a stakeholder request surge. The ideal candidate will have performed 3-5 years of front end and backend secure development, have a strong knowledge of web application vulnerabilities and remediation techniques, and at least one or two security certifications. We would like someone who is comfortable communicating with our developers at their level, be able to remediate security vulnerabilities rather than adding to the team's workload, and be able to be an integral part of the development team.

b. What percentage of time with this FTE spend designing, coding, unit testing, cross-training, and starting application security?

Initially, this FTE will be focused 100% on application security and then eventually may transition or split time on other tasks depending on workload and needs.

c. How will the FTE's combined roles balance the pressure of meeting development deadlines with the need to prioritize security?

As you know, the legislature has a relatively small IT team and team members are required to wear multiple hats and do what's best for the project and business. There is currently a need for separate security and developer positions on a full time basis. However, in the interest of limiting the budget request, both positions have been rolled into one. While the security role will take precedence and is the primary responsibility of this position, they will be pressed into development if the need and urgency arises to meet deadlines. Having a security person embedded into the development team will also help with integrating application security in the team's processes. Over time, as this position matures and the teams evolve, this position may evolve as well.

As stated earlier, the priority is application security and then Java development.

d. Will the new application security changes only apply to the Java development team, or across all software development platforms under LIS's purview? Please provide the scope.

New application security changes will translate across all technology stacks and systems as applicable. This role may fix vulnerabilities in Java based applications specifically, but the goal is to work with all platforms.

15. Please provide more information about the request for a Ruby on Rails developer, who will also implement a DevOps methodology, including new processes, procedures, and tools.

a. What is the Ruby on Rails experience needed for this position, including the number of years coding custom applications? What is the DevOps experience needed for this position, including the number of years driving and managing DevOps changes?

The primary role for this position is working with all platforms to develop a DevOps strategy. Ruby on Rails experience will likely only be used during a surge in stakeholder requests. The ideal candidate will have 3-5 years of DevOps experience and 1-3 years of Ruby on Rails experience. The DevOps background is far more important than the Ruby on Rails experience. We are currently performing DevOps differently across all platforms and it is resulting in inefficiencies and rework.

b. What percentage of time with this FTE spend designing, coding, unit testing, cross-training, and starting application security in the department?

This role will work with the Application Security Analyst to develop and implement a secure DevOps strategy. The percentage of time working Application Security will depend on the strategy.

c. Will the new DevOps changes only apply to the Ruby on Rails development team, or across all software development platforms under LIS's purview? Please provide the scope.

DevOps changes will be implemented across all software development platforms as applicable. Some tools may scale better across platforms than others and may require different approaches. The DevOps resource will work with the development teams from each platform to plan and implement our DevOps strategy.

16. Please provide the rationale for choosing DevOps implementation in lieu of DevSecOps methodologies. Please also include the existing status of LIS' DevOps efforts. What is LIS's change management plan for implementing DevOps methodologies?

We will be building the foundation for DevOps and App Security in parallel. We're not choosing DevOps over DevSecOps. DevSecOps methodologies will be incorporated as we build that foundation. We will perform a cost/benefit analysis on any recommendations before implementation. We will prioritize the work in conjunction with our stakeholder needs.

17. Is Java being used to develop new applications, or only to maintain legacy systems? If new applications are being developed in Java, please explain the approach.

Currently, two applications (XDOME and CLIMBS) are being built using the Java Spring framework. These two applications are getting built using a decoupled architecture, where the front end is being built using React.js. iLegislate and LCS' Research Request system are two existing Java applications in production and require ongoing maintenance (including adding new functionality).

18. The request outlines several recently completed, current, and future applications, projects, initiatives, and ongoing improvements.

a. How are these items prioritized?

Items are prioritized based on decisions made on the basis of urgency in terms of technology obsolescence or lack of expanding functionality, business need, resources needed, IT staff turnover, loss of critical business resources, business process changes, effort, etc.

b. Please list all the current and, if known, future projects the LIS plans to assign to the new FTEs and those projects' statuses.

Application Security Implementation and DevOps Implementation are new projects that have not started because we need the resources to start them. These projects will be the priority for the new FTE. However, they may be assigned to the following applications, if workload allows:

> XDOME, CLIMBS, CGA Website Rewrite, Visitor Services, CLUVS Rewrite. There is a large backlog of new features for iLegislate, LCS Research Requests application and ongoing change requests for the CDC/JTC Requests application.

19. The request explains that existing staff "is responsible for transitioning existing applications from obsolete technologies into new technology." The request further explains that staff is "committed to developing a strong Java and Ruby on Rails team."

    Does the department have a current inventory of its obsolete technology, and an active plan for addressing any issues? Please summarize and provide the status.

    There is a list of applications and technology identified for modernization. Some are in the process of transition, others are slated in the near future and others are slated for later consideration. There are various reasons for modernizing, including but not limited to: a shrinking technology ecosystem, lack of commercial or open source support, lack of internal resources to support, consolidation of technology stacks, and improved functionality with new technology. In some cases, digital transformation by automating or eliminating existing manual processes is the reason for change.

    Some examples of applications and technologies identified for modernization or digital transformation are:

    - The chamber voting system (CLUVS);
    - The Colorado General Assembly Website;
    - the Budget Management system (CLIMBS);
    - the use of WordPerfect for bill drafting;
    - The email system; and
    - Visitor Services Tours system.