2020 PRIORITIZATION OF CYBERSECURITY AND LEGACY SYSTEMS (PCLS) MODERNIZATION PROJECTS

INSTRUCTIONS FOR TEXAS STATE AGENCIES

PUBLISHED 6/25/2020

SUBMISSION DEADLINE: AGENCY LAR SUBMISSION DATE

TEXAS DEPARTMENT OF INFORMATION RESOURCES

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

Section 2054.069, Government Code entitled *Prioritized Cybersecurity and Legacy Systems Projects Report* requires the Texas Department of Information Resources (DIR) to report on state agency cybersecurity projects and projects to modernize or replace legacy systems, as defined by Section 2054.571, Government Code to the Legislative Budget Board (LBB) no later than October 1 of each even-numbered year.

DIR relies on PCLS Project Questionnaires to develop the required list of prioritized projects. This document provides general instructions for completing these questionnaires. Agencies will use the DIR SPECTRIM portal to submit their PCLS Project Questionnaire responses. Only PCLS Project Questionnaires submitted through the SPECTRIM portal by the submission deadline will be considered for prioritization.

PURPOSE

The PCLS Project Questionnaire provides agencies with the opportunity to demonstrate the risks and potential impacts of failing to address their cybersecurity and legacy modernization projects. DIR will use the responses provided in the PCLS Project Questionnaire along with the Application Portfolio Management (APM) assessment responses of the business applications associated with the project in determining the project prioritization that will be sent to the LBB in October 2020.

QUESTIONNAIRE ORGANIZATION

The 2020 PCLS Project Questionnaire is organized as follows:

- **Part 1: General Information** asks general information about the project, the agency's legislative appropriation request.
- **Part 2: Business Process and Application Information** asks the agency to link the specific associated business applications and processes that would be impacted by the request.
- **Part 3: Cybersecurity Issues and Controls** asks the agency for a description of cybersecurity threats, vulnerabilities, controls, procedures, and other safeguards that are currently in place.
- **Part 4: Legacy Issues** gathers information concerning legacy requests, including items being refreshed, the business value of impacted systems, and the expected return on investment.
- **Part 5: Probability Determination** gathers information to determine the likelihood of a failure in the event the project is not funded.
- **Part 6: Impact Determination** gathers information to determine potential impact in the event the project is not funded.

Note that certain parts of the questionnaire are required depending on the type of project selected:

Cybersecurity Projects – Parts 1, 2, 3, 5, & 6.

Legacy Projects – Parts 1, 2, & 4.

GENERAL INSTRUCTIONS

SENSITIVE INFORMATION

Section 2054.069(c), Government Code states that "a state agency shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information contained in or written, produced, collected, assembled, or maintained in connection with the report under Subsection (a). Section 552.007 does not apply to information described by this subsection."

Additionally, Section 552.139, Government Code, provides an exception to the Texas Public Information Act regarding the confidentiality of information related to security or infrastructure issues for computers. Information that relates to computer network security, design, operation, or defense of a computer network, may be treated as confidential. DIR will comply with the Texas Public Information Act and all applicable statutes in protecting state computing systems. DIR will produce two PCLS Prioritization Reports – a non-sensitive public version, and a confidential version for the appropriate state leadership audience.

COLLECTION TOOL

LOGGING IN

The Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) is a secure web-based governance, risk, and compliance platform administered by DIR. Each agency Information Security Officer (ISO) and Information Resources Manager (IRM) are provided with accounts and additional users can be added upon request.

To access the SPECTRIM portal navigate to the following URL and enter your appropriate credentials. If you do not have an account, you can have an existing account holder open an archer support request form within the portal to have an account created for you. Users requesting access must have authorization from the agency ISO, IRM, or their authorized delegate.

Note: the reset password function will not work for inactive/locked accounts. If you attempt a password reset and don't receive an automated email shortly after, chances are your account is inactive and you will need to email GRC@dir.texas.gov or have someone open an archer support request on your behalf to have your account reactivated. Support requests can be initiated by clicking on the "support request" link on the top of every page in the "quick links" section.

URL: https://dir.archer.rsa.com/Default.aspx

Username: your agency email address

It may be helpful to bookmark the portal login page for future reference. Only one user will be able to edit a record at a time. All data entered is saved in a central database and may be viewed and updated in future sessions during the reporting period. After logging in, you will be directed to a different home page depending on your organizational role. The home page can be changed to whichever dashboard you prefer by selecting "edit" in the upper left corner of your home dashboard.

CREATING A PCLS PROJECT QUESTIONNAIRE RECORD

At the top of the portal there is a banner for groups of applications called workspaces. The PCLS Project Questionnaire workspace is titled "PCLS."

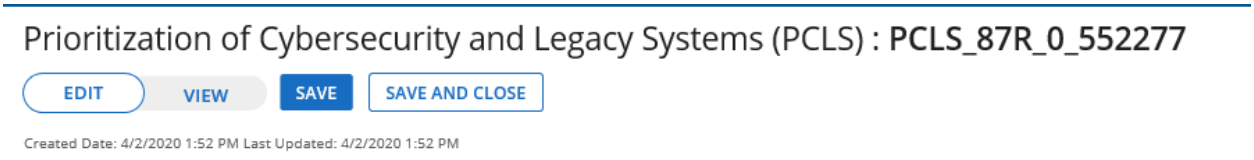
If you click directly on the workspace tab, you will be redirected to the PCLS Dashboard. Additionally, you can click on the dropdown caret next to the workspace name to see the component applications/questionnaires. If you want to navigate directly into the listing of PCLS records. If the PCLS Workspace tab is not available, you may have to click the vertical ellipsis at the right of the banner to view additional workspace options.

On the PCLS Dashboard, there are additional resources/reports to assist with tracking progress. To create a new PCLS Project Questionnaire, select the "New Cybersecurity/Legacy LAR Prioritization Record" in the PCLS Links section. If you want to see previous year's submissions or return to an existing questionnaire, select "View All (Past or Present) PCLS Records and select the PCLS Tracking Key (e.g. PCLS_87R_123456) of the questionnaire.

After selecting "New Cybersecurity/Legacy LAR Prioritization Record," the system will prompt you to select your organization. For most users there will only be one option but be sure to select the appropriate organization for the target PCLS Project Questionnaire if you have multiple organizational associations.

Once the record is created, certain fields will automatically populate, and a unique ID called the PCLS Tracking Key will be generated. **This PCLS Tracking Key will need to be submitted with your agency Legislative Appropriations Request (LAR) through the LBB's ABEST System.**

At the top of the PCLS Project Questionnaire you will see several action buttons. If the response options are not displaying, you may be in "view" mode and will need to select "edit" to enable the ability to respond to questions. If the selection for these options is grayed out, you do not have the appropriate access and will need to either be assigned as a delegate by the PCLS Project Questionnaire submitter or contact GRC@dir.texas.gov to resolve the issue.

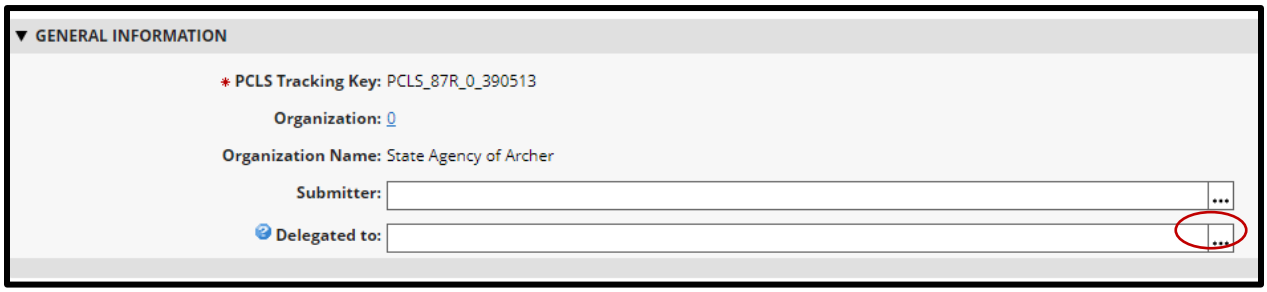


Additionally, at the top of the record you have the option to either save or save and close the record. You must at least populate the project name (question 1.01) field before being able to save the record. Saving the record will save any progress but will allow you to stay in the current record. Save and close will save the progress but will also

close the record and direct you to the previous page. If you want to close a record without saving changes you can select the "x" in the upper right-hand corner to take you to the previous page.

ASSIGNING A DELEGATE OR REVIEWER

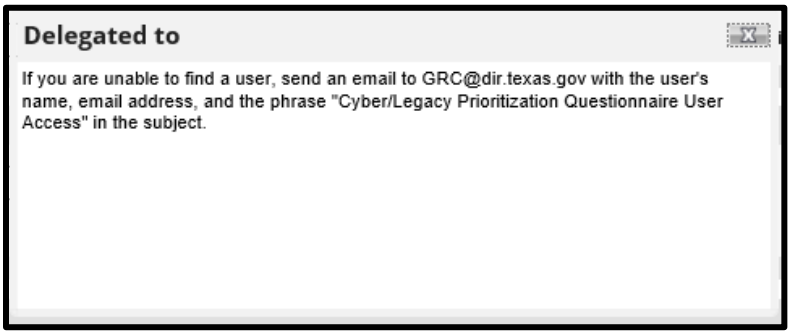
The record creator is the default submitter. If the record creator wishes to allow other active users to edit information, they can look-up the user in the "delegate to" field by clicking on the ellipsis. If a user does not appear in the lookup dialog box, they either do not have an existing account, or their account is inactive. Contact GRC@dir.texas.gov if you are unable to find a user in the delegate field.



You can also assign a reviewer in the general information section. Assigning a reviewer is an optional process that will allow a user to review the PCLS Project Questionnaire responses prior to submitting the questionnaire to DIR.

HELP TEXT & COMMENTS

A blue question mark icon next to a field indicates that there is help text relating to that field. If you click on the icon, a dialog box will open with more information about the field.



You may add question specific comments or attach supporting evidence for your answers by clicking on the yellow sticky note icon next to each question. Once you have saved the comment, the icon will change to a darker color yellow to show that a comment has been added.

PROJECT TYPE

Within the Part 1 section of the PCLS Project Questionnaire, you will be asked to identify the type of project being requested. Depending on your selection, certain sections of the questionnaire will be displayed. Be sure to select the appropriate project type based on the guidance provided in the questionnaire outline of this document.

LINKING BUSINESS APPLICATIONS

Part 2 of the PCLS Project Questionnaire asks the agency to link business applications that are being impacted by the PCLS Project. These associations are important to determine the prioritization of a given project. During the 2020 Information Resources Deployment Review (IRDR), agencies were asked to inventory their business applications and determine whether to perform an APM assessment on a given business application. The responses to those APM assessments factor into the prioritization methodology of a given PCLS Project through the associations made in this part of the PCLS Project Questionnaire.

***NOTE**: Business applications that have not had an APM assessment performed or have not had an APM assessment performed within the last four years will not be available to be selected to associate with a PCLS Project Questionnaire. To ensure that the appropriate business applications are linked, agencies should identify the business applications that are impacted by a given PCLS Project and complete an APM assessment on the application as needed.*

To link the impacted business applications, select “lookup” on the right side of the Part 2 section and select the applicable applications.

Multiple applications can be selected at once by checking the box next to each application. To select an entire page of applications, you can select the check box in the header row of the lookup table. Be aware that applications may span several pages, and the select all option using the header row only selects the records on the page being displayed. To select more applications not displayed, you will need to navigate to the additional pages using the page selection at the bottom of the lookup table.

SUBMISSION

SPECTRIM QUESTIONNAIRE SUBMISSION

Once you have completed all the required fields, the submitter or their delegate will have the ability to change the submission status. You may keep the PCLS Project Questionnaire in the "In Process" action state until you are ready for finalization. When you have completed the PCLS Project on the new PCLS LAR item, change the PCLS Agency Action to "Finalize". The system will flag all the required items with an asterisk. Once you save, after setting the “PCLS Agency Action” to “Finalize”, the system will display a message indicating any missed required fields. If this occurs, complete the missing required fields, and save the record again. This will route the PCLS Project to the proper reviewer, if applicable. If you finalize and leave a required field blank, the system will flag those with a red asterisk (*). Please populate the fields, set the PCLS Agency Action to “Finalize,” and then “Save and close” record.

LEGISLATIVE APPROPRIATIONS REQUEST SUBMISSION

All Cybersecurity and Legacy Modernization System funding requests considered for this LAR period must be entered prior to the agency LAR due date. The PCLS Tracking Key generated by SPECTRIM for the PCLS project must be submitted in context with the Agency’s LAR related funding requests.

The Legislative Appropriations Request (LAR) instructions for the 87th Legislative Session will require agencies with projects that are identified for the Prioritization of Cybersecurity and Legacy Systems Projects (PCLS) report to identify the PCLS Tracking Key in 4.A. Exceptional Item Request Schedule and 5.B. Capital Budget Project Information.

QUESTIONNAIRE STATUSES

Not Started – initial status indicating that the PCLS record has been created, but no questions have been completed.

In Process with Submitter – questionnaire record has been saved, but content has not been submitted for next stage. The submitter or delegate can come back to the record and update responses in this stage.

Awaiting Business Application Assessment(s) – the questionnaire has business applications associated in Part 2 that do not meet the required criteria to be included in the project questionnaire. Associated applications must have the required application fields completed (e.g. Mission Critical) and must have an APM assessment completed on the application within the last 4 years. The agency will need to either complete the required APM assessment(s) or exclude applications that do not meet the requirements to submit the questionnaire.

In Process with Reviewer – indicates that the questionnaire record has been finalized by the submitter and is awaiting review. This stage will only occur if the submitter or delegate assign someone to the optional reviewer field. The reviewer will need to review the questionnaire record to approve or reject the questionnaire back to the submitter.

Rejected by Reviewer / Re-Finalize – indicates the optional reviewer has rejected the questionnaire. The submitter or delegate will need to revise the questionnaire content and re-finalize to submit for review again.

Awaiting Submission to LBB – indicates that the PCLS questionnaire has successfully been submitted to DIR via SPECTRIM. The record questionnaire content will become read-only at this time. Once the PCLS Tracking Key has been submitted via the agency's LAR, the submitter will need to return to the PCLS questionnaire record and update the "Project submitted to LBB with its PCLS Tracking Key" field to "Yes" and populated the "Date Submitted to LBB" field.

PCLS Tracking Key Submitted to LBB – indicates that the PCLS questionnaire submission has been fully submitted to both DIR and LBB. Most of the record will become read only, but users may still update information about the project including Funding Status and Project Status.

Not Submitted – Archived – indicates that the PCLS record was created during a previous legislative session and was not indicated as submitted to LBB. The record is read-only and may not be updated. If users want to submit the request for the 87th legislative session, they will need to create a new PCLS record.

SUPPORT

COMMUNICATIONS

DIR will use the tx-irm mailing list for primary communications regarding the PCLS Process. Additional information can be found on the PCLS Webpage.

SUPPORT AND ASSISTANCE

- For general inquiries about PCLS content (e.g. question clarification, process questions) email pcls@dir.texas.gov.
- For support with the SPECTRIM portal (e.g. password resets, obtaining credentials) email grc@dir.texas.gov or open an archer support request from within the portal.

PART 1 – GENERAL INFORMATION

1.01 Project Name: Enter the Legislative Appropriations Request (LAR) Item Name.
<Enter a text response>

1.02 Project Narrative: Provide a description of the project.
<Enter a text response>

1.03 Project Type:

- Cybersecurity (Parts 1, 2, 3, 5, 6)
- Legacy Modernization (Parts 1, 2, 4)

Cybersecurity Projects must possess at least one of the following criteria:
►The project's primary purpose must be improving the organization's cybersecurity or enhancing the organization's capability to identify, detect, protect, respond, or recover from cybersecurity threats and vulnerabilities. ►The project must have clear objectives that will improve the organization's cyber maturity as measured in the biennial information security plan.
Legacy Modernization Projects must possess at least one of the following criteria:
►The project's primary purpose must be modernizing the agency's legacy systems as defined in Sec. 2054.571, Government Code. "Legacy system" means a computer system or application program that is operated with obsolete or inefficient hardware or software technology. ►The project must also be intended primarily to support continued systems currency through monitoring the agency's application portfolio and IT infrastructure.

1.04 Dollars Requested: Total Project IT Dollars requested for the biennium (enter a number)
$_____

1.05 Matching Funds: Is this project subject to time-sensitive federal or other matching funds?

- Yes
- No

1.05a Matching Expiration: When do the matching funds expire?
<Enter a date>

1.06 Existing Project: Is this request part of an existing PCLS project?

- Yes
- No

1.06a Prior PCLS/LAR Request(s): Please Link to an existing PCLS LAR Request(s).
<Use lookup and select one or more>

1.06b Existing Project Name: If project(s) not found, please provide the name of the existing project(s).
< Enter text response >

1.06c Existing Project Funding: What aspects of the existing project(s) have been funded already and for what amount?
<Enter text response>

1.07 Distinct Project Funding: Is this project directly associated with other distinct project funding request(s) sponsored by your agency or another for this legislative session?

- o Yes
- o No

1.07a Distinct Project Name: List the names of those projects:
<Enter text response>

1.08 Multiple Sessions: Can the project be broken down across different legislative sessions?

- o Yes
- o No

1.09 Impact if Not Funded: If this project is not completed in the next biennium, what will be the impact?
<Enter text response>

1.10 Previous Denial: Has this project been previously denied?

- o Yes
- o No

1.10a Denial Summary: Please provide a short summary with the corresponding session(s).
<Enter text response>

1.11 Is this an exceptional item request?

- o Yes
- o No

1.12 Business Drivers: What are the business drivers related to this project request? Check all that apply.

Strategic Alignment – Project meets a State Strategic Goal as designated in the State Strategic Plan or an agency/division goal.

Statutory Fulfillment – State/federal requirements, new legislation.

Tactical Necessity – Those projects that are necessary to maintain existing services/systems (e.g. software upgrades).

Financial Optimization/Efficiency – Enables cost savings. Provides cost savings through efficiencies, optimization of processes, expenses, or resources.

Remediation – Remediate audit findings or vulnerabilities (e.g. Sunset Report, State Auditor's Office Report).

- ☐ Strategic Alignment
- ☐ Statutory Fulfillment
- ☐ Tactical Necessity
- ☐ Financial Optimization/Efficiency
- ☐ Remediation
- ☐ Other (write in)
- ☐ None of the above

1.13 Service Category: What government sectors/services does this project address? Check all that apply.

- ☐ Courts
- ☐ Electricity
- ☐ Education
- ☐ Emergency Services
- ☐ Environmental Protection
- ☐ Health Care
- ☐ Military
- ☐ Public Transportation
- ☐ Public Facilities
- ☐ Public Safety
- ☐ Social Services
- ☐ Telecommunications
- ☐ Urban Planning
- ☐ Transportation Infrastructure
- ☐ Waste Management
- ☐ Water Supply Network
- ☐ Other (write in)
- ☐ None of the above

1.14 Project Complexity: Which of the following best describes the level of complexity associated with the project?

Simple – straightforward, project can be implemented using internal knowledge and skillsets.

Moderate – moderate resources and expertise required, may include few systems or third parties.

Complex – significant resources and expertise required, may include a few systems or third parties and dependencies.

Very Complex – significant resources and expertise required, including many systems or third parties and dependencies.

- o Simple
- o Moderate
- o Complex
- o Very Complex

1.15 Project Duration: Which of the following best describes the project duration?

Duration of the project should be defined by the date which the work begins, i.e. excluding "request-for" or statement-of-work processes and the date the project deliverables are accepted.

Short – less than 6-month implementation.

Moderate – 6 months to 1-year implementation.

Long-term – 1 to 2-year implementation.

Extended – over 2-year implementation.

- o Short
- o Moderate
- o Long-term
- o Extended

1.16 Timing Importance: Which of the following describes the project timing importance?

Immediate – if not funded, there is greater than a 25% chance that significant risk/adverse impacts will be realized over the biennium or the project addresses critical existing vulnerabilities/weaknesses or relieves major impacts on current resources and service delivery.

Short-term – if not funded, there is less than a 25% chance that significant risk/adverse impacts will be realized over the biennium or the project addresses significant existing vulnerabilities/weaknesses or relieves significant impacts on current resources.

Mid-term – if not funded, there is less than a 10% chance that significant risk/adverse impacts will be realized over the biennium.

Long-term – if not funded, there is less than a 5% chance that significant risk/adverse impacts will be realized over the biennium.

- o Immediate
- o Short-term
- o Mid-term
- o Long-term

1.17 Benefit Realization: Which of the following best describes the time to realize the full benefits/return on investment of the project?

Immediate – the benefits associated with this project will be immediately realized upon completion of the project.

Short-term – the benefits associated with this project will be realized within 6 months of the completion of the project.

Mid-term – the benefits associated with this project will be realized within 6 months to 1 year of the completion of the project.

Long-term – the benefits associated with this project will be realized in 1 to 2 years of the completion of the project.

Extended – the benefits associated with this project will be realized in over 2 years of the completion of the project.

- o Immediate
- o Short-term
- o Mid-term
- o Long-term
- o Extended

1.18 Does this project meet the criteria for a Major Information Resources Project?

"Major information resources project" means: (A) any information resources technology project identified in a state agency's biennial operating plan whose development costs exceed $5 million and that: (i) requires one year or longer to reach operations status; (ii) involves more than one state agency; or (iii) substantially alters work methods of state agency personnel or the delivery of services to clients; and any information resources technology project designated by the legislature in the General Appropriations Act as a major information resources project.

- o Yes
- o No

PART 2 – RELATED BUSINESS APPLICATIONS

Business Applications Note:

Business Applications were identified during the IRDR. A Business Application name is the high-level label used by an agency business and IT organization to easily identify a group of functions provided by one or more systems to accomplish the specific business needs of the agency. A Business Application is typically a combination of integrated hardware and software (including data and applications), internally developed custom systems, commercial off the shelf (COTS) applications, and/or customized third-party systems. Information systems include interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications, and people.

APM Assessment Note:

Business Applications must have an APM assessment performed within the last 4 years to be associated to a PCLS project. If you do not see the Business Application you are attempting to associate in the lookup values in SPECTRIM, then the application may not have an associated APM assessment completed that meet the criteria.

2.01 Business Applications being directly refreshed/replaced/migrated/modernized as part of this project:
<lookup – select all that apply>

2.02 Other related applications indirectly impacted by the project:
<lookup – select all that apply>

2.03 This project impacts the entire application portfolio of the agency, e.g. the project will enhance the security of all the agency's business applications.

- Yes
- No

PART 3 – CYBERSECURITY ISSUES AND CONTROLS

3.01 Cybersecurity Issues: Provide a brief description of the issue, including threats (sources or causes of disruption) and vulnerabilities (weaknesses in systems or services) associated with this risk.
< Enter text response >

3.02 Cybersecurity Controls: Identify current safeguards, controls, or procedures that mitigate (lessen) the risks associated with this project not being funded.
< Enter text response >

PART 4 – LEGACY ISSUES

4.01 Modernization Benefits: Describe the benefits from modernization, with metrics to be used by the agency for tracking Return on Investments (ROI).

< Enter text response>

4.02 Methodology: Provide an explanation of the methodology used to identify the benefit and cost values, i.e. quantify the benefit (refer to similar QAT requirements as identified in the Project Delivery Framework Business Case Workbook).

< Enter text response>

4.03 Project Total Costs (Enter a number)

$_____

4.04 Project Total Benefit (Enter a number)

$_____

4.05 Project Breakeven Point. Select the option for when the benefits are expected to outweigh the costs.

- o 1-3 Years
- o 4-6 Years
- o 7-10+ Years

4.06 Project Expected Return on Investment

- o Greater than 70%
- o Between 20-69%
- o Less than 20%

4.07 Which of the following are intended benefits of the project? Check all that apply.

- ☐ The project reduces agency staff or allows staff reassignment through efficiencies (e.g. requiring fewer staff to complete work, reducing/eliminating manual processes, reducing turnaround time).
- ☐ The project improves/reduces the use of existing resources (hardware, software, runtime).
- ☐ The project improves the agency's ability to increase collections or other revenue generation.
- ☐ The project results in a new service that provides additional value to a constituent or a prospective employer.
- ☐ The project results in a lower cost of transacting services for constituents.
- ☐ The project results in a service being available at more convenient times (e.g. 24x7) or more locations.
- ☐ The project results in a greater ease of use for constituents because of fewer interactions required and presentation is organized around consumers.
- ☐ The project results in constituents having their needs met with fewer contacts to government or fewer interactions with government employees.
- ☐ Other (write in)

4.08 Servers: Select the number of physical servers being refreshed and/or replaced.

- 0
- 1-5
- 6-10
- 11-15
- 16-20
- 21-25
- 26-30
- 31-40
- 41-50
- More than 50 (write in)

4.09 Virtual Servers: Select the number of virtual servers being refreshed and/or replaced.

- 0
- 1-5
- 6-10
- 11-15
- 16-20
- 21-25
- 26-30
- 31-40
- 41-50
- More than 50 (write in)

4.10 Software: Select the number of legacy or near end of life software components being refreshed and/or replaced.

- 0
- 1-5
- 6-10
- 11-20
- 21-30
- 31-50
- 51-100
- 101-200
- 201-300
- More than 300 (write in)

4.11 Upgrade Costs: Identify the estimated cost to upgrade associated software instances that are out of support and at risk from a security perspective. (enter a number)
$_____

4.12 System Attributes: Please identify the attributes of the system(s). Select all that apply to the project.
□ An internal application for agency uses
□ Business-to-business
□ Citizen-facing and impacting constituents (*answer 4.12a)*

4.12a Describe the impact on the people of Texas/constituents affected by this project.
<Enter text response>

4.13 Does this project involve migration of existing applications or infrastructure to a cloud environment?

- ○ Yes, private cloud
- ○ Yes, hybrid cloud
- ○ Yes, public/government cloud
- ○ No (*skip 4.13a)*

4.13a Describe the extent of cloud services usage in this project.
<Enter a text response>

4.14 Does this project involve migration from a mainframe infrastructure?

- ○ Yes
- ○ No

PART 5 – PROBABILITY DETERMINATION

5.01 Which of the following best describes the threat capability needed to exploit the vulnerabilities/weaknesses addressed by this project?

Very Low – The vulnerabilities/weaknesses could be exploited through human error or with little to no technical expertise (bottom 2% when compared against the overall threat population).

Low – The vulnerabilities/weaknesses could be exploited with minor technical skills/abilities (bottom 16% when compared against the overall threat population).

Moderate - The vulnerabilities/weaknesses could be exploited with moderate technical expertise (average skill and resources (between bottom 16% and top 16%).

High – The vulnerabilities/weaknesses require moderate to significant technical expertise (top 16% when compared against the overall threat population).

Very High – The vulnerabilities/weaknesses require significantly advanced technical expertise and time to be exploited (top 2% when compared against the overall threat population).

- Very Low
- Low
- Moderate
- High
- Very High

5.02 Which of the following best describes the incentive for someone to obtain unauthorized access to, or disrupt the functionality of, the data and information within the systems that this project is addressing?

Very Low – there is no apparent incentive or very minor incentive for someone to obtain unauthorized access to the data and systems that this project is addressing.

Low – there is a small incentive, monetarily or otherwise, to obtain unauthorized access to the data and systems that this project is addressing. The risk-reward trade-off for malicious actors is not significant.

Moderate – there is a moderate incentive, monetarily or otherwise, to obtain unauthorized access to the data and systems that this project is addressing. Unauthorized access may provide a pivot point to more valuable data or systems. The risk-reward trade-off for malicious actors is moderately significant.

High – there is a high incentive, monetarily or otherwise, to obtain unauthorized access to the data and systems that this project is addressing. Unauthorized access to data could potentially provide direct value to malicious actors.

Very High – There is very high incentive, monetarily or otherwise, to obtain unauthorized access to the data and systems that this project is addressing. Unauthorized access to data could provide significant monetary value or leverage to malicious actors.

"Someone" may refer to a disgruntled associated, former associate, contingent worker, member, cyber attacker, competitor, or others.

- Very Low
- Low
- Moderate
- High
- Very High

5.03 How effective are existing controls (as noted in question 3.02) at decreasing the likelihood of exploiting the vulnerabilities addressed by this project?

Not Effective – existing controls do not significantly reduce the likelihood of exploiting the vulnerabilities/weaknesses addressed by this project (only protects against bottom 2% of an average threat population).

Somewhat Effective – existing controls reduce the likelihood of exploiting the vulnerabilities/weaknesses addressed by this project by a small amount (only protects against bottom 16% of an average threat population).

Moderately Effective – existing controls reduce the likelihood of exploiting the vulnerabilities/weaknesses addressed by this project by a moderate amount (protects against the average threat agent).

Effective – existing controls reduce the likelihood of exploiting the vulnerabilities/weaknesses addressed by this project by a significant amount (protects against all but the top 16% of an average threat population).

Very Effective – existing controls reduce the likelihood of exploiting the vulnerabilities/weaknesses addressed by this project by a very significant amount (protects against all but the top 2% of average threat population).

- Not Effective
- Somewhat effective
- Moderately Effective
- Effective
- Very Effective

5.04 Which of the following best describes the reliability of existing controls (as noted in question 3.02) in relation to decreasing the probability of vulnerabilities/weaknesses being exploited and mitigating the impacts of exploiting the information assets associated with this project?

Unreliable – existing controls have not been effectively tested/verified or are often subject to failure (0-20% reliable).

Somewhat Reliable – existing controls have been tested/verified but may be subject to failure (20-80% reliable).

Moderately Reliable – existing controls have been tested/verified and are unlikely to fail under normal circumstances (80-90% reliable).

Reliable – existing controls have been tested/verified and are subject to failure under significantly abnormal circumstances (90-95% reliable).

Very Reliable – existing controls are regularly tested/verified, and control contingencies/redundancies are in place to mitigate risks of potential control failures (95-100% reliable).

- Unreliable
- Somewhat Reliable
- Moderately Reliable
- Reliable
- Very Reliable

5.05 Which of the following best describes the frequency in which threat actors attempt to access/disrupt the information assets associated with this project?

Very Low – Less than .1 times per year (less than once every 10 years).

Low – between .1 and 1 times per year.

Moderate – between 1 and 10 times per year.

High – Between 10 and 100 times per year.

Very High – More than 100 times per year.

- Very Low
- Low
- Moderate
- High
- Very High

5.06 Which of the following best describes the exposure of the vulnerabilities/weaknesses being addressed by this project?

Internal non-privileged – the vulnerabilities/weaknesses being addressed by this project are only accessible from within the agency's network.

Internal privileged – the vulnerabilities/weaknesses being addressed by this project are only accessible from within the agency's network with additional privileged/administrative access.

External – the vulnerabilities/weaknesses being addressed by this project are accessible from outside of the agency's network, e.g. internet-facing.

Internal and External – the vulnerabilities/weaknesses being addressed by this project are accessible from both inside and outside the agency's network.

- Internal Non-privileged
- Internal Privileged
- External
- Internal and External

PART 6 – IMPACT DETERMINATION

6.01 Which of the following best describes the impacts on reputation if the vulnerabilities/weaknesses being addressed by the project were exploited?

Negligible – there would be no significant risk to reputation of the organization or management.

Minor – the reputation of the organization and executive management would most likely not be adversely impacted or may only be temporarily affected. Executive management would likely be retained, and the event would not likely obtain media attention.

Moderate – the reputation of the organization and executive management would likely be called into question without long-term or permanent damage. Executive management may be dismissed, and the event may obtain minor (local/regional) media attention.

Significant – the reputation of the organization and executive management would be damaged in the short and long-term. Executive management would likely be dismissed, and the event would likely obtain significant (e.g. national, widespread) media attention.

Critical – the reputation of the organization and executive management would be significantly damaged in the short and long-term. Executive management would likely be dismissed, and the event would obtain significant (international, widespread) media attention. Organizational credibility and citizen trust would be irreparably damaged for the foreseeable future.

- Negligible
- Minor
- Moderate
- Significant
- Critical

6.02 Which of the following best describes the impacts on productivity/operations if the vulnerabilities/weaknesses being addressed by the project were exploited?

Negligible – There would be no significant risk of disruption to productivity/operations.

Minor – Normal operations could be restored by existing resources within acceptable limits of recovery time objectives.

Moderate – Normal operations could be restored within acceptable limits of recovery time objectives. Restoration may require additional resources or assistance.

Significant – Normal operations could be restored beyond acceptable limits of recovery time objectives. There may be a noticeable lapse in the delivery of mission critical services.

Critical – Normal operations could be restored beyond acceptable limits of recovery time objectives. Significant downtime of mission critical services would occur. External assistance would likely be required to restore operations.

- Negligible
- Minor
- Moderate
- Significant
- Critical

6.03 Which of the following best describes the impacts on public safety if the vulnerabilities/weaknesses being addressed by the project were exploited?

Negligible – There would be no significant risk of bodily harm or death to the population.

Minor – There would be a small risk that the impacts could result in bodily harm to a small segment of the population.

Moderate – There would be a small to moderate risk that the impacts could result in bodily harm to a small segment of the population.

Significant – There would be a small to moderate risk that the impacts could result in bodily harm to a large segment of the population.

Critical – There would be a small to moderate risk that the impacts could result in bodily harm or death to a large segment of the population.

Catastrophic – There would be a significant risk that the impacts could result in widespread bodily harm or death to the population.

- Negligible
- Minor
- Moderate
- Significant
- Critical
- Catastrophic

6.04 Which of the following best describes the potential impacts of fines and judgments levied if the vulnerabilities/weaknesses being addressed by this project were exploited or not remediated?

Negligible – There would be no significant risk of fines or judgments resulting from the exploitation of the vulnerabilities/weaknesses being addressed).

Minor – There is a small risk that minor fines and judgments would occur. Fines and judgments would not exceed an amount that would cause excessive strain on agency resources).

Moderate – There is a moderate risk that minor fines and judgments would occur, or a small risk that moderate fines and judgments would occur. Fines and judgments may cause excessive strain on agency resources or the agency's capability to deliver mission critical services).

Significant – There is a significant risk that large fines and judgments would occur. Fines and judgments would likely cause a significant strain on agency or state resources and disrupt the agency's capability to deliver mission critical services).

Critical – There is a significant risk that large fines and judgments would occur. Fines and judgments would exceed the agency's resources and require emergency state intervention.

- Negligible
- Minor
- Moderate
- Significant
- Critical

6.05 How effective are existing controls (as noted in question 3.02) at mitigating the impacts of exploiting the vulnerabilities/weaknesses being addressed by this project?

Not Effective – existing controls do not significantly reduce the loss exposure of the information assets associated with this project (0-10% reduction in total potential loss).

Somewhat Effective – existing controls reduce the loss exposure of the information assets associated with this project by a small amount (10-20% reduction in total potential loss).

Moderately Effective – existing controls reduce the loss exposure of the information assets associated with this project by a moderate amount (20-60% reduction in total potential loss).

Effective – existing controls reduce the loss exposure of the information assets associated with this project by a significant amount (60-80% reduction in total potential loss).

Very Effective – existing controls reduce the loss exposure of the information assets associated with this project by a very significant amount (80-100% reduction in potential loss).

- o Not Effective
- o Somewhat Effective
- o Moderately Effective
- o Effective
- o Very Effective

6.06 Which of the following best describes the ***largest potential**** single event loss magnitude (response costs, replacement costs, reputation costs, operational costs, etc.) if the vulnerabilities/weaknesses addressed in this project were exploited?

**Largest possible loss should be considered as the total costs in terms of dollars potentially to occur directly relating to the event. Agencies should take into consideration existing controls and capabilities for detection, response, and recovery relating to security incidents as well as data sensitivity and impacts of system downtime.*

o $0 - $10k o $10k - $100k o $100k - $1M o $1M - $10M o +10M

6.07 Which of the following best describes the ***smallest potential**** single event loss magnitude (response costs, replacement costs, reputation costs, operational costs, etc.) if the vulnerabilities/weaknesses addressed in this project were exploited?

**Smallest possible loss should be considered as the total costs in terms of dollars most likely to occur directly relating to the event. Agencies should take into consideration existing controls and capabilities for detection, response, and recovery relating to security incidents as well as data sensitivity and impacts of system downtime.*

o $0 - $10k o $10k - $100k o $100k - $1M o $1M - $10M o +10M

6.08 Which of the following best describes the ***most probable**** single event loss magnitude (response costs, replacement costs, reputation costs, operational costs, etc.) if the vulnerabilities/weaknesses addressed in this project were exploited?

**Most probable loss should be considered as the total costs in terms of dollars most likely to occur directly relating to the event. Agencies should take into consideration existing controls and capabilities for detection, response, and recovery relating to security incidents as well as data sensitivity and impacts of system downtime.*

o $0 - $10k o $10k - $100k o $100k - $1M o $1M - $10M o +10M