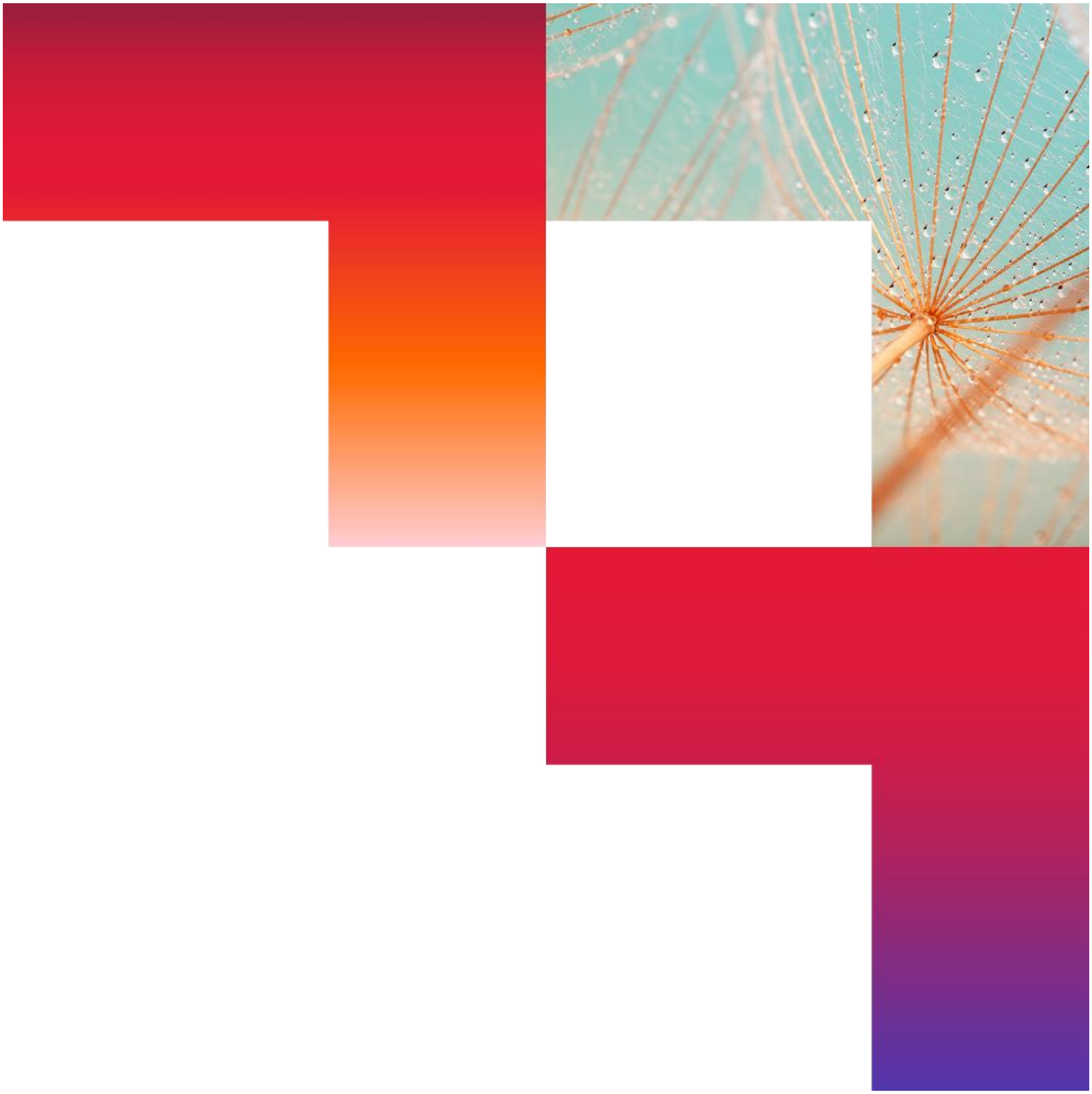


Response to RFQ

State Integrated Recovery Operations and Management Systems (SIROMS)

State of New Jersey Department of Community Affairs

2025-02-19

CGI

PROPRIETARY AND CONFIDENTIAL

The information contained in this document may be proprietary and confidential to CGI and/or to the receiving party. This document cannot be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, without the written approval of CGI. The receiving party is exempt from this restriction for evaluation purposes only.

If you have received this document by mistake, note that the reading, reproduction, or distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at 703-267-8000 and to return this document by certified mail.

The information in this proposal is submitted on 2025-02-19 on behalf of CGI by the following authorized representative: Timothy Hurlebaus.

Timothy Hurlebaus
President and Chief Operating Officer
CGI
11325 Random Hills Road, 8th Floor
Fairfax, VA 22030
Tel: 703-267-8000

CGI

CGI
11325 Random Hills Road, 8th Floor
Fairfax, VA 22030
Tel: 703-267-8000

cgi.com

2025-02-19

Lauren Rebovich

State of New Jersey Department of Community Affairs

Division of Disaster Recovery and Mitigation

101 S. Broad St.

Trenton, NJ 08608

Subject: State Integrated Recovery Operations and Management Systems (SIROMS)

Dear Ms. Rebovich,

The enclosed proposal is submitted in response to the above-referenced RFQ.

We have carefully read and examined this RFQ and have conducted such other investigations as were prudent and reasonable in preparing the proposal. We agree to be bound by the statements and representations made in this proposal and to any agreement resulting from the proposal.

Yours truly,

Timothy Hurlebaus

President and Chief Operating Officer

1 TABLE OF CONTENTS

Table of Exhibits

1 Executive Summary

Since June 2013, CGI has had the privilege of partnering with the State of New Jersey Department of Community Affairs, Division of Disaster Recovery and Mitigation (DCA-DRM) to maintain and enhance the State Integrated Recovery Operations Management System (SIROMS). During the initial phase of implementing the Superstorm Sandy action plan, CGI was charged with developing a system that would, among other things, immediately support the processing of funds to applicants and enable partner agencies to track and report on the delivery and progress of recovery programs.

When the COVID-19 pandemic halted the economy and Hurricane Ida devastated New Jersey infrastructure again, CGI remained DCA-DRM's recovery partner of choice. SIROMS was enhanced to centralize the collection, management, and reporting capacity of grant program and funding data from multiple sources. Unique modules were developed to capture data for COVID-19 transparency and reporting purposes. As part of this effort, CGI also supported the development of an interactive transparency portal, for the Governor's Disaster Recovery Office, to provide citizens insights into allocated and disbursed COVID funds.

Leveraging an existing baseline module to reduce cost and time, multiple program modules have been developed to support New Jersey citizens with their recovery from Hurricane Ida. New online registration and application submission functionality allow citizens to more easily learn about and apply for relief. An online portal for eligible applicants supports electronic submission of required documentation and ongoing communication between applicants and the agency regarding the status of their project. Home inspections are scheduled electronically and can now be conducted with a mobile application implemented to streamline the process and reduce agency overhead.

Having played a key role in the evolution of SIROMS, CGI is uniquely qualified to continue maintaining and hosting SIROMS. We are pleased to be able to commit resources to this project that have years of experience and insight having worked side by side with DCA-DRM through its evolution from solely Sandy relief to being a central organization supporting disaster recovery across the State. These CGI Partners, some of which have been on SIROMS since 2013, have unparalleled knowledge of SIROMS from both the functional and technical perspectives and can be mobilized on day one of the contract, helping to ensure continuity of service and reducing the downtime associated with other vendors.

1.1 Why CGI?

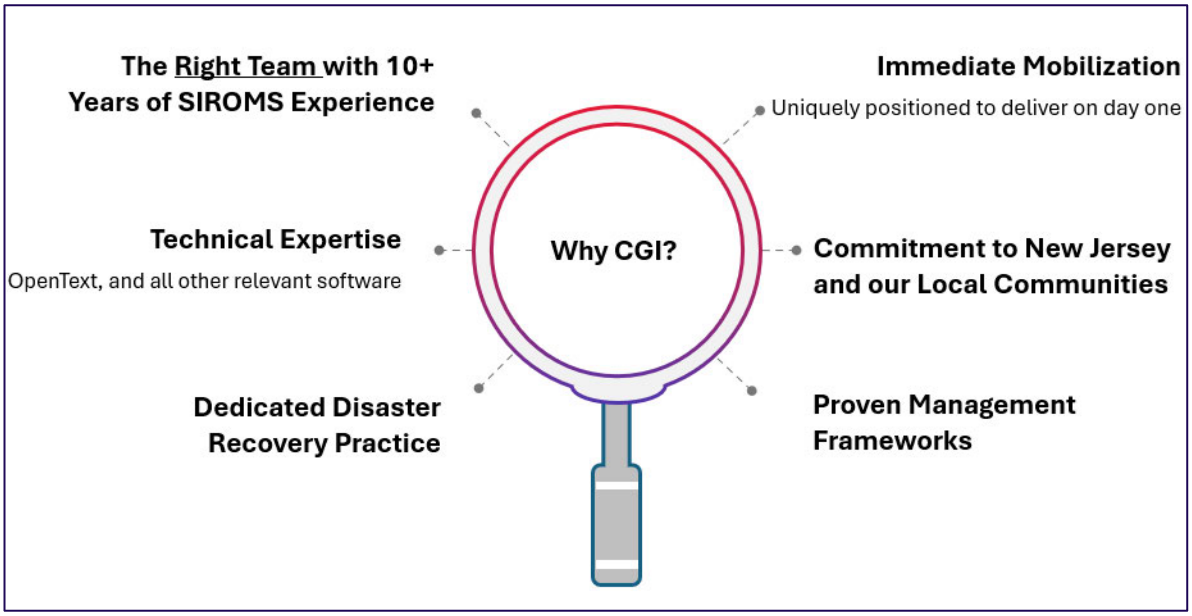
Founded in 1976, CGI is among the largest independent IT and business consulting services firms in the world. It was recently awarded the TIME World's Best Companies recognition, demonstrating its success in balancing stakeholder interests, serving as a partner and expert of choice for our clients, and employer of choice for our CGI Partners. CGI was also again ranked by Forbes as a top management consulting firm in 2024, based on the insights-driven business and strategic IT consulting services we deliver to commercial and government clients.

TIME
WORLD'S
BEST
COMPANIES
IN PARTNERSHIP WITH statista 2024

Forbes 2024
AMERICA'S BEST
MANAGEMENT
CONSULTING FIRMS
POWERED BY STATISTA

With more than 90,000 professionals working in 400 locations across the globe, CGI provides comprehensive, scalable, and sustainable IT and business consulting services that are informed globally and delivered locally. This means CGI has the resources and experience to appropriately scale project teams up or down as projects change, and manage and support the largest, most complex applications.

CGI intentionally leverages an organizational structure and operating model that directs decision making, promotes leadership, and hires and retains consultants in proximity to our clients. This means all projects operate under our New Jersey Business Unit and are delivered by primarily local resources; the same resources that have been by your side and working behind the scenes to make SIROMS the highly regarded system that it is today. This is the team with the institutional disaster recovery knowledge and the technical know-how to implement your vision for the next phase of SIROMS.



Why CGI?

The Right Team with 10+ Years of SIROMS Experience

Immediate Mobilization

Uniquely positioned to deliver on day one

Technical Expertise

OpenText, and all other relevant software

Commitment to New Jersey and our Local Communities

Dedicated Disaster Recovery Practice

Proven Management Frameworks

1.2 CGI's History of Success Supporting New Jersey

With 45+ years of government experience and a 30+ year established partnership with the State, CGI knows New Jersey. We bring best practices and a collaborative mindset to help organizations achieve their modernization goals. The many successful partnerships CGI holds within the State, including that with DCA-DRM, are displayed below.

DCA
NJ Department of Community Affairs
Department of Transportation
The State of New Jersey
NJ Office of Information Technology
Department of Environmental Protection
New Jersey
State of New Jersey
Department of the Treasury
Cats
powered by njoit
Department of Children and Families
Ocean County
New Jersey
City of Newark
Incorporated 1836

CGI has a long history of success providing qualified IT professionals for state and local government agencies across New Jersey. With extensive New Jersey State government experience, strong organizational support, a comprehensive management and delivery approach, and a wealth of professional resources, CGI will continue to provide DCA-DRM the right team of local disaster recovery professionals committed to supporting the next phases of SIROMS.

CGI has engaged in the delivery of dependable solutions including:

- State Integrated Recovery Operations and Management System (SIROMS) - New Jersey Department of Community Affairs (DCA-DRM)
- Mainframe Remediation Project – New Jersey Office of Information Technology (OIT)
- New Jersey Environmental Management System - New Jersey Department of Environmental Protection (DEP)
- Child Welfare Solution - New Jersey Department of Children and Family Services (DCF)
- eCATS Timekeeping Solution - Office of Information Technology (OIT)
- NJSTART – The Department of Transportation (DOT)
- CGI Advantage – New Jersey Ocean County
- COVID Data Pipeline - City of Newark

CGI is excited to continue our strong, longstanding partnership with the Department of Community Affairs. We anticipate we will exceed the State's expectations through the ongoing maintenance and hosting of SIROMS. Leaders across the State have trusted CGI to provide better quality systems to help government and industry work better for the residents of the State. **Our commitment to exceed the expectations of our clients is demonstrated by an overall 9 out of 10 client satisfaction score**, reported directly by our clients through in-person satisfaction assessment sessions. CGI attributes this high rating to a hands-on delivery approach that allows us to build long-term valued professional relationships with our clients. Furthermore, as a publicly traded company, over 90% of our employees (whom we refer to as Partners) own shares in the firm, which demonstrates a commitment to CGI's success and the success of our clients.

1.3 CGI's Disaster Recovery Practice

With over fifteen years of focused disaster recovery data management services, CGI is uniquely qualified to provide the advisory, consulting, delivery, and management support services necessary to maintain and host SIROMS. CGI combines the size and experience of a large global corporation with the agility and execution of a highly focused disaster recovery practice. This experience is reflected in our delivery of positive recovery results in Louisiana (Katrina and Gustav), New Jersey (Sandy, Ida, and COVID-19), and Puerto Rico (Irma, María, the 2020 Earthquake Cluster, COVID-19, and Hurricane Fiona) – spanning the most damaging natural disasters in United States history.

In response to the needs of local governments administering these disaster recovery programs, CGI has developed the only comprehensive financial and grant management data system to manage grantee/recipient/state-side responsibilities for the two largest sources of federal disaster recovery funding. CGI's Disaster Recovery Practice has implemented solutions in various forms for specific disasters including the State Information Recovery Operations and Management System (SIROMS), which manages HUD CDBG-DR, FEMA MAP, and ARPA programs for the State of New Jersey, and the Puerto Rico Disaster Recovery Solution (PR DRS) which manages FEMA programs for the Government of Puerto Rico (GPR).

CGI's Disaster Recovery Practice is the right choice for the following reasons:

- As the designers, architects, and developers of disaster recovery systems, CGI is uniquely capable of continuing to provide the level of maintenance and customization required by the State of New Jersey.
- CGI's Disaster Recovery solutions have supported the ongoing audit and regulatory compliance efforts in Louisiana, New Jersey, and Puerto Rico, facilitating the successful completion of multiple direct system audits from FEMA, HUD, and other oversight entities.
- CGI's Disaster Recovery solutions have been proven as the trusted system of record for recovery efforts of over $60 billion.
- CGI's broad business knowledge of FEMA and HUD programs provides DCA-DRM with the necessary support to implement recovery and action plans.
- CGI has assembled a uniquely qualified, proven team of local partners, technology partners, and federal regulatory experts to deliver for DCA-DRM.
- CGI has facilitated and fostered sharing of best practices and exchange of expertise across our various Disaster Recovery and Grant Management support initiatives.

1.4 CGI is Committed to the Local Community

CGI has continuously demonstrated its commitment to New Jersey. We have been in New Jersey for over thirty years and maintain an office in the heart of New Brunswick, with approximately 200 partners, to help ensure that our leadership and resources can provide a rapid response to our clients in the state. CGI has swiftly grown our local team to prepare for initiatives here in New Jersey. Over the last two years, CGI has made investments through our collegiate recruitment program, bringing over two dozen new graduates to the New Jersey team.

P·TECH
Pathways in Technology
Early College High School

Furthermore, as an industry partner to the New Brunswick School District, CGI introduces children to STEM fields as early as elementary school through our STEM@CGI program. CGI also encourages them to join a P-TECH school to acquire the academic, technical, and workplace skills needed for a successful IT career. A team of our early career CGI Partners, who graduated in the last five years, mentor P-TECH students for the four to six years they spend in the program.

Students have the opportunity to shadow our consultants and senior consultants during the summer, attend internal meetings, and sign up for a paid internship when they turn eighteen. These activities enable the P-Tech students to gain real-world corporate experience. This will continue to familiarize the students with CGI's culture and work, should they choose to join us after they graduate. As Mike Reagan, Senior Vice-President, Consulting Services, U.S. East Operations, summarizes: "They can hit the ground running from day one with the real-world experience they gained working side by side on our project teams." These are just a few of the reasons why CGI was named one of New Jersey's Best Places to Work by NJBIZ for the last three years and was recognized as a Top Workplace in 2024 by NJ.com.

NJBIZ
Best Places to Work
NJ
2023

TOP WORK PLACES 2024

nj.com + Jersey's BEST

2 Solution Approach

2.1 Management Overview

Having worked hand-in-hand with DCA-DRM for over ten years in support of the State's execution of Superstorm Sandy, COVID-19, Hurricane Ida, and Mitigation Assistance programs, CGI is the only team with a comprehensive understanding of how the State's recovery efforts have grown and evolved to-date and what the State still aims to accomplish. Through this experience, our team has also built invaluable relationships with DCA-DRM and other State agency/entity stakeholders responsible for the day-to-day execution and administration of the disaster recovery efforts, allowing us to tailor and refine our approach to the management of the SIROMS project to best meet the needs of DCA-DRM and its partners. This section, and its subsections, will detail our approach towards the management of the SIROMS project which has been shaped and molded by these relationships and the countless hours expended by our team of disaster recovery professionals towards designing, developing, testing, implementing, enhancing, and maintaining SIROMS to date. These subsections serve to supplement our proprietary Client Partnership Management Framework (detailed in Section 2.1.1) that defines our overall approach to project management which is shared and right-sized globally across all projects managed by CGI.

2.1.1 Contract Management

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Exhibit 1 - CGI's Client Partnership Management Framework

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted] [redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

Exhibit 4 - CGI's CPMF Components and Relationships

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

[redacted]

2.1.2 Contract Schedule

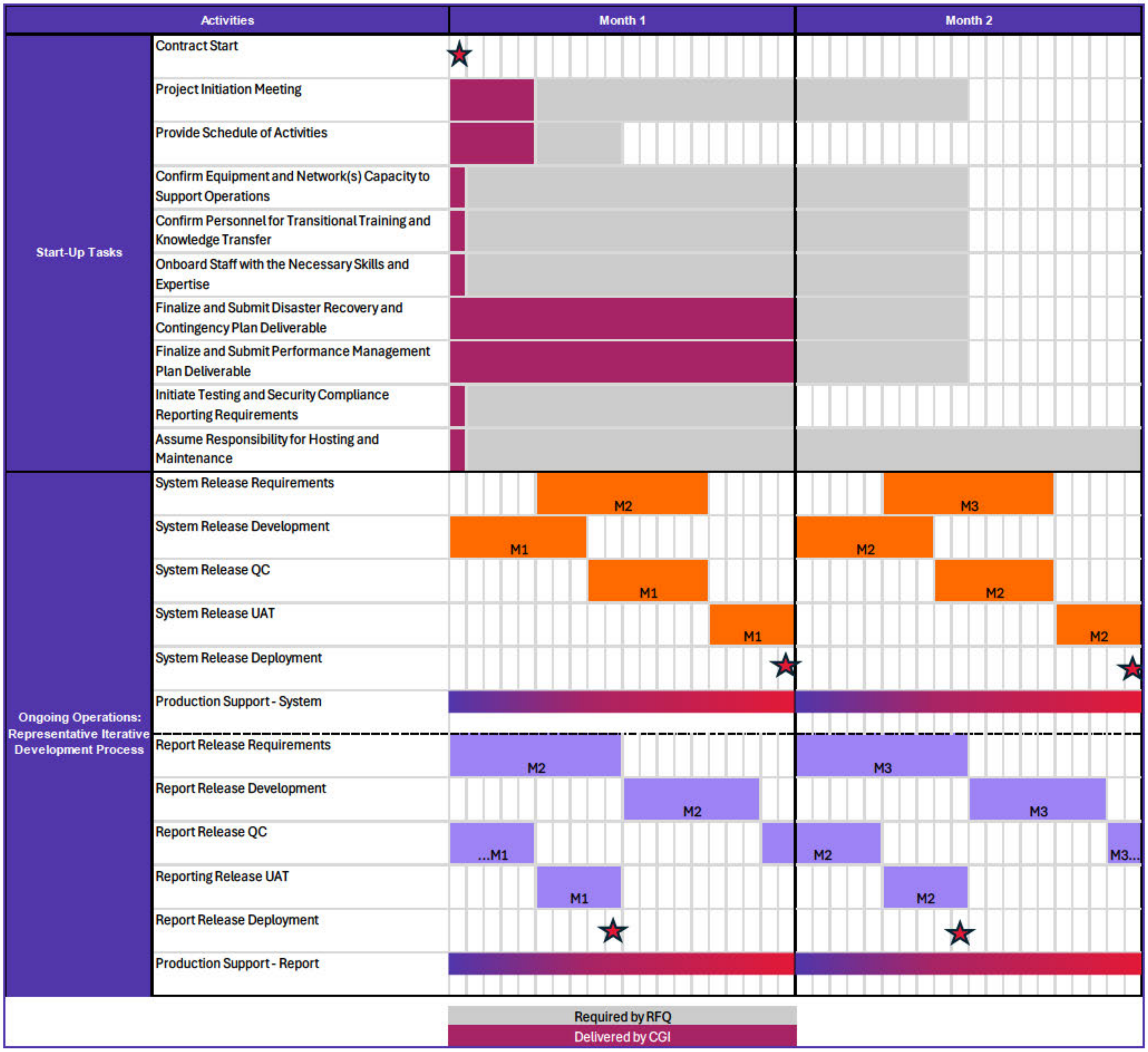
The schedule below represents the anticipated timeline for both project initiation tasks as well as the ongoing maintenance and enhancement of SIROMS. As indicated throughout this response, CGI will exceed DCA-DRM's expectations for completing start up tasks during the mobilization period. CGI is ready for business on day one of the contract and will immediately put the right team to work finalizing start-up deliverables while simultaneously carrying on with the ongoing operations of the system, without the delays associated with any other vendor.

For the ongoing maintenance and enhancement of SIROMS, CGI anticipates that the primary schedule used for the SIROMS project will be the release calendar. The release calendar defines when each major system release will be held, which will typically be every 4-5 weeks. Given our success over the past 10+ years, we propose the continuation of our hybrid Agile methodology in which we work collaboratively with DCA-DRM to set the release date and determine which major pieces of functionality, documented through the Change Request process, are included in the release. The release calendar includes dates for determining which Change Requests will be scoped, when BFRDs are due to DCA-DRM for review, and when DCA-DRM approval is required to maintain the release schedule. In addition, CGI will work with DCA-DRM to schedule user testing sessions, helping to ensure that key stakeholders have an opportunity to review, test and provide feedback on the upcoming system changes before they are implemented in the production environment.

Throughout the release cycle, CGI will also work with DCA-DRM to schedule any high-priority help desk tickets that are too critical to wait until the scheduled release date and prioritize other fixes for the actual release. In the event of an off-cycle request, DCA-DRM will notify CGI that a bug fix or change is high-priority and will provide a desired production deployment date. CGI will in good faith work to achieve the requested timeline but will communicate with DCA-DRM should the timeline not be achievable. In these instances, CGI will provide alternatives that could address the situation, which may include temporary fixes, or changes to the release scope to address the more urgent need. In any event, it will be a joint effort between CGI and DCA-DRM to determine the best course of action for resolving the issue.

In conjunction with the system release calendar, another major drive of work will be the reporting release schedule. Typically, the report release lags the system release by two weeks to allow for table structure updates to stabilize and propagate to the data warehouse. Like the system release calendar, CGI will work collaboratively with DCA-DRM to set the release date and determine which reports will be developed or modified in a given release. Dates will be established for when BFRDs are due to DCA-DRM for review, when DCA-DRM approval is required to maintain the release schedule and when reports should be delivered for user testing. Deviations to the schedule will be communicated to DCA-DRM and the teams will jointly work to address any issues or concerns.

Exhibit 5 - SIROMS Schedule



2.1.3 Mobilization Plan

CGI understands the importance of a swift and effective mobilization towards the maintenance of SIROMS. CGI implemented the original SIROMS and continues to enhance the solution on a regular basis, working in close partnership with DCA-DRM PMO. Given the fact that we are currently mobilized and actively working to maintain and enhance the SIROMS system, our mobilization effort will be seamless and will leverage key personnel who have existing long-term experience with SIROMS as far back as 2013 and its various user groups. Because our experience with SIROMS and its user base is proven, CGI is the lowest risk candidate for this request and is well positioned to provide the highest and fastest return on investment.

At CGI, it is in our DNA to approach each engagement with an approach that is flexible, collaborative, and responsive to rapidly evolving client needs and priorities. This approach has helped us build lasting client relationships and earn the role of a true trusted advisor to multiple State of New Jersey entities, such as DCA-DRM, NJDEP, and Ocean County. This strength has been exemplified by the recent successful implementation of DCA-DRM's Disaster Recovery and Mitigation Portal, a comprehensive and modular platform that has enabled the DCA-DRM team newfound flexibility in their program administration process. By providing a framework that can be leveraged to enhance active programs, as well as administer entirely new programs, CGI has bolstered the mobilization ability of DCA-DRM for the long term. We will take this same collaborative approach with DCA-DRM to help ensure that the mobilization period lays the foundation for successful continued partnership in the next chapter of the SIROMS project.

The following table lists key activities of our mobilization plan; additional detail on the schedule for mobilization tasks can also be found in section 2.1.2.

Exhibit 6 - Key Mobilization Activities

Mobilization Activity	Description
Assemble Key Personnel	**Day 1:** Our Key Personnel are well positioned to provide all services required by the RFQ. Not only do they have breadth of experience with SIROMS, but are familiar with DCA-DRM's existing processes, and will integrate seamlessly into established business practices. While many other vendors would likely have to squander precious time trying to identify resources, procure resources with CDBG-DR experience, and make a new office space operational, CGI's established experience with the system will enable us to hit the ground running.
Facilitate Project Initiation Meeting	**Day 1- 5:** An important milestone of the Project Mobilization Plan is the Project Initiation Meeting, which is required to occur no later than thirty (30) calendar days after receipt of notification to award contract. The meeting will take place at DCA-DRM and will be attended by key personnel from CGI and DCA-DRM, including the State Contract Manager (SCM). Additionally, the meeting will provide an opportunity for DCA-DRM to ask for clarification of various aspect of CGI's proposal, including (but not limited to) CGI's approach to managing this contract and project management methodology. While CGI is excited to facilitate the Project Initiation Meeting as the official kickoff of project-related activities and collaboration between DCA-DRM and CGI, we would also like to emphasize that CGI will be available to facilitate various other meetings with DCA-DRM stakeholders throughout the mobilization period. CGI's New Jersey headquarters in New Brunswick allows our staff to be readily accessible to work with DCA-DRM's project team, and we look forward to taking advantage of our close proximity to DCA-DRM to collaborate in preparation for a successful project kickoff.
Establish Governance and	**Day 1:** Project governance is an essential component to any successful IT project, particularly an initiative that requires

Mobilization Activity	Description
Status Reporting Structure	coordination between multiple state agencies, and collaboration with local government entities. CGI has successfully established a tiered approach to project governance at each of our active New Jersey projects, enabling project issues to flow upwards and downwards incrementally, so that the appropriate stakeholder group may address them. Typically, straightforward, tiered approach to governance allows approximately 85% of issues to be resolved by "on-the-ground" Project Teams, while 10% of issues are addressed by a Management-level Steering Committee, and the remaining 5% are addressed by an Executive-level Steering Committee. In addition to our tiered governance framework, CGI recommends deploying other cross-functional forums on an ad-hoc basis to facilitate decision-making and oversight in certain critical areas, depending on the phase and evolution of the project. CGI will prepare and facilitate a weekly status meeting with the State Contract Manager. The purpose of this meeting will be to discuss the detailed project status, including release schedules, and provide additional updates on all outstanding high-priority items. Additionally, CGI will provide a weekly status report to the State Contract Manager and other stakeholders as required that details the following: • Key Milestones in the coming weeks • Current project risks • Current project issues • Release schedule • Significant accomplishments in the reporting period • Infrastructure updates • Reporting updates • Look ahead scheduled out of office
Recruit and Onboard Project Team Members	**Day 1:** CGI understands that project success ultimately depends on the quality of the functional, technical, and management professionals that are committed to the project. As mentioned earlier, CGI will assign resources that have created, implemented, and maintained SIROMS for years, granting us the unique advantage of possessing the most resources with the best understanding of the system. Since we do not foresee the need to recruit or onboard new resources, we are confident we can hit the ground running on day one. In the event that additional resources need to be recruited, CGI will leverage its established talent acquisition process, detailed in Section 2.3.2
Procure Hardware, Software, and Essential Equipment	**Day 1:** Based on our understanding of the RFQ requirements, CGI requires no immediate equipment, inventory, supplies or materials to begin work on the SIROMS project. Should the need to procure arise during the project implementation, CGI will follow its procurement

Mobilization Activity	Description
	model to buy the necessary hardware and software items as required for maintaining the SIROMS system specified in the RFQ. The procurement process begins with DCA-DRM describing the potential need including preferred vendors to address the described need to the CGI PM. The CGI PM will research options to resolve the need, including reaching out to additional vendors to gather additional documentation or setup demonstrations with DCA-DRM. If requested, CGI may provide a presentation on the merits of each vendor and score the vendors according to the known requirements. CGI will confirm the vendor is an approved CGI third party vendor and factor that in the scoring system as it may impact procurement. Once DCA-DRM has settled on a decision to proceed, the CGI PM will start negotiations with the vendor and retain a quote. The CGI PM will also provide an estimate to DCA-DRM for the completion of the procurement for evaluation. Once the quote is approved by DCA-DRM, CGI will procure on behalf of the agency.

PLAN FOR DEPLOYING KEY PERSONNEL

CGI understands that a productive and successful mobilization period depends on the availability and commitment of Key Personnel to help get the project off the ground. CGI is fortunate to have a pre-assembled team of highly skilled Partners with many years of SIROMS experience. Their experience, combined with their industry expertise, will position SIROMS to hit the ground running. During the mobilization period, all Key Personnel referenced below will begin executing elements of Project Mobilization Plan immediately of notification of intent to award the contract.

The table below provides a list of Key Project Team Members that will be available for the duration of the mobilization period, including their corresponding Project Role, and a high-level plan for how each individual will be utilized to support activities throughout the mobilization:

Exhibit 7 - Key Mobilization Team Members

Name	Project Role	Functionality
Vaid Ram	Engagement Manager/Project Manager	• Co-facilitator of the Project Initiation Meeting • Oversee execution of Project Mobilization Plan activities • Approve revisions to Project Schedule, Project Management Plan, and new hires of any Key Personnel • Approve procurement of any software, hardware, or other essential equipment • Single point of contact for SCM and DCA DRM • Manage CGI's mobilization team

Name	Project Role	Functionality
		• Coordinate day-to-day mobilization activities • Assess the need for new hires, and coordinate recruitment, interview, and hiring activities with H.R. Recruitment Team • Serve as PMO advisor during the Project Initiation Meeting, and support revisions to the Project Management Plan
Tom Rispoli	Application Delivery	• Manage CGI's technical mobilization team • Serve as technical advisor for application systems during the Project Initiation Meeting • Support revisions to technical components of the Project Schedule and Project Management Plan • Perform final interview for new hires of technical resources as needed. • Provide support to SCM and DCA-DRM for any questions or clarification re: technical components of the proposal
Diana Goldin	Functional/QC	• Manage CGI's functional mobilization team • Serve as functional advisor during the Project Initiation Meeting • Support revisions to the functional components of the Project Schedule and Project Management Plan • Perform the final interview for new hires of functional resources as needed. • Provide support to SCM and DCA-DRM for any questions or clarification re: functional components of the proposal • Maintain consistency across Disaster Recovery products and facilitate sharing across teams
Madhu Chandran	Database and Business Intelligence	• Manage CGI's database and reporting mobilization team • Serve as technical advisor for reporting systems during the Project Initiation Meeting • Support revisions to the reporting/database components of the Project Schedule and Project Management Plan • Perform the final interview for new hires of technical resources as needed. • Provide support to SCM and DCA-DRM for any questions or clarification re: technical components of the proposal • Serve as database, data warehouse and reporting advisor during the Project Initiation Meeting, and support revisions to the Project Management Plan
Steve Ramroop	Helpdesk	• Serve as Helpdesk advisor during the Project Initiation Meeting, and support revisions to the Project Management Plan

Name	Project Role	Functionality
Scott Bowers	Infrastructure Architect	• Serve as infrastructure advisor during the Project Initiation Meeting, and support revisions to the Project Management Plan

2.2 Functional Requirements

2.2.1 Cloud Computing Business Process Management (BPM) Systems

CGI built SIROMS using proven technologies, such as Business Process Management (BPM), and Microsoft .NET, to meet the fast moving and scalable needs of a Disaster Recovery program. The core of the back-office functionality of SIROMS is built upon the OpenText Metastorm BPM product. **MBPM provides workflow-driven management of the business processes of any DR program or administrative function, providing clear visibility into the progress, status, and task ownership for any given record.** BPM also facilitates rapid system design and development; this allows us to reuse specific modules and use these building blocks to build additional financial and grant management solutions, as needed. CGI has utilized the .NET Framework on components of the solution which require less complex workflow and greater flexibility from a User Interface (UI) perspective. **Utilizing a hybrid agile approach to the Software Development Life Cycle (SDLC), with a focus on deep collaboration with program management and staff**, CGI will continue to work with DCA-DRM for maintenance of SIROMS and phased implementation of any changes required by DCA-DRM.

CGI and DCA-DRM have worked closely together over the last few years to add several new innovative components to SIROMS to extend the capabilities of the system:

- The ability to easily add configurable “details” pages to SIROMS modules. These details pages can have new fields easily added by updating configuration. This allows updates to these pages to be performed quickly and without requiring a code deployment.
- A configurable applicant portal that allows registered applicants to communicate with DCA staff, upload/download documents, and request payments for their applications.
- A mobile inspection application that allows inspectors to record findings while on site visits, even when internet access is not available at the inspection site.

CGI looks forward to working with DCA-DRM on future innovations to the SIROMS system.

The underlying SIROMS technology suite consisting of OpenText MBPM, Microsoft BI, .NET and Tableau dashboards will continue to help in designing and implementing solution that DCA-DRM needs. CGI will continue to leverage the following capabilities within SIROMS:

- The OpenText MBM suite consists of a graphical design studio, an application processing engine, a .NET web portal for both desktop and mobile browsers integration tools for optional client development in .NET or Java, and components for use in SharePoint.
- A process management engine designed to drive the progression of work in structured or unstructured processes or cases; the BPM platform in SIROMS has a comprehensive rules engine that allows implementation of workflows with dynamic roles and conditional action to allow the end user to determine the path of the process

- A graphical model-based environment for designing processes and supporting activities; CGI has integrated standalone .NET components within the BPM framework to create user-friendly interfaces and flexible user designs
- The combination of MBPM's graphical workflow definition capabilities and the table-driven framework that CGI and DCA-DRM developed for validations and dynamically created fields can be utilized to quickly update the business rules that are implemented by the system. CGI's years of experience with MBPM and their in depth understanding of the table drive frameworks gives them the ability to leverage these capabilities to their maximum potential starting on day one of the contract.
- Integration with OpenText Content Server for document management capabilities to store files such as PDF documents and images in compliance with the record retention requirements established in the RFQ
- MBPM's graphical workflow management tool table driven field generation framework allows for role specific access to the system's various components to be rapidly configured
- Ability to link processes to the resources they control such as proposals, grant activities, grantees and fund disbursements; Data captured through form interaction are stored in the repository along with the relevant system generated information about the process such as status, current assignment, and event history
- Web-based interaction portals that allow staff and grantees to interact with the processes they are involved in; SIROMS has customized the To Do and Watch lists to help users understand the tasks that are assigned to them and require action for continuation in a process
- Tighter integration with external application and data sources; SIROMS has multiple integration points with NJCFS, NJDEP, Standard ACH File Format, Housing contractor systems and also with other internal data sources
- Active analytics reports and dashboards, using SSRS and Tableau for monitoring and improving operational performance in areas such as processes, resources, grant activities and fund balances.
- Management and administration. The SIROMS solution includes a management portal for administering users, roles, and deployed processes. These administrative forms allow for the delivery of user supported business rule settings, search interfaces, management of lookup tables, etc.
- Reporting, dashboards and visualizations to provide decision support for program stakeholders and data feeds using SQL Server Reporting Services and Tableau.
- Exportable data in common formats for ETL processes and advanced analytics using SQL Server Integration Services
- Configurable interfaces delivered through Apache Camel allow SIROMS to connect to various third-party systems. See section 2.2.2 for further details.
- CGI has unparalleled experience and understanding of the SIROMS architecture and underlying technologies. We know the database layout, the frameworks, the tools and the business reasons behind the system functions. This allows us the ability to rapidly make any changes needed to maintain or enhance the system and support the system data.
- ESRI Arc GIS for spatial reporting needs that support GIS maps using SIROMS data.

2.2.2 Interfaces

The SIROMS integration services are built on Apache Camel and Windows scheduled tasks, to construct and implement interfaces and integration across disparate systems. They provide the flexibility and simplicity necessary to implement and manage interfaces with various data sources hosted by other State departments/authorities and third-party contractors. These tools can be configured to be triggered by external events or run on predefined schedules.

Hosting integration services in AWS allows us to continue to support integrations through scanners, FTP, emails, database connections, XML based with web services, and RESTful APIs as well as new options like communicating with applicants through text messages via AWS Simple Notification Service (SNS). Over the life of the SIROMS project, CGI has implemented internal and external integrations for various purposes like sending close out notifications to applicants, executing account transfers with Bank of America via standard ACH file format, transferring inspection information with the Department of Environmental Protection and importing funds requests. CGI is ready to work with DCA-DRM to automate future interactions with external entities. Leveraging AWS will allow CGI to keep communicating with applicants, business users, external applications, and internal systems on secure reliable hardware as well as provide new avenues for communicating with external parties.

The following interfaces are currently implemented through SIROMS:

- Treasury A1
  - Purpose – Transmit Funds Request information to the NJCFS system for payment.
  - Type – FTP send
  - Schedule: Daily
  - Supported Grant Management Programs:
    - Funds Request
  - Successfully completed transactions to date:
    - 66,062 Checks and counting
- Treasury WREC/OPVL
  - Purpose – Receive Check Number, Check Date, and Check Status information from NJCFS.
  - Type – FTP receive
  - Schedule: Daily
  - Supported Grant Management Programs:
    - Funds Request
  - Successfully completed transactions to date:
    - 66,062 Checks and counting

In addition to the above interfaces. We have successfully supported the following interfaces.

- Securely transmit SIROMS data to contractors through contractor's web services.
  - Interface 71, DEP (Completion)
- Securely receive external data from contractors to SIROMS through web services.
  - Transmissions Interface 7, 8, IDONE
- Securely transmit files between SIROMS and third parties through FTP, SFTP service.
- Import and export data from DRGR, US Treasury (UST) and HAPPY System using a combination of FTP and ETL processes.
- CSV file with PER and other ARPA transaction details are uploaded to UST using the ETL file generation process. This process scans the database for ARPA data and creates more than 500 individual csv files.

- Transfer funds from homeowner and CDBG escrow accounts to Homeowner, builder, NJCFS, and GFI accounts through Bank of America
- Sending email notifications to their proper recipients through STMP email service
  - All active programs (AMP, PER, ARP-QPR, GMR, IDA, MAP, and TBRA etc.) Stages and Status information
- Offline processes for SIROMS reports through SIROMS web services.
  - Folder Creations, Folder Stage Moves for QPR, GMR, IDA, MAP, TBRA, and ARP-QPR etc.
- Offline processes for SIROMS Data Reports through the SQL Server Reporting Service.
  - Invoke SSRS report process to generate reports, such as Forecasting Summary Reports, Forecasting Detail Reports, and QPR reports etc., and send it to requester through SMTP email.

2.2.3 Helpdesk

The SIROMS Helpdesk has significant experience over the previous eleven (11) years working with DCA-DRM end users providing Tier 1 support and understands the important role of Helpdesk when called upon to respond to an incident. It is our belief that when a user reaches out for assistance, the SIROMS Helpdesk will be ready and available to either resolve the reported issue (Tier 1) or route it appropriately and efficiently to CGI teams with the requisite subject matter and/or technical expertise (Tier 2/3).

SOFTWARE

SIROMS Helpdesk staff currently use, and will continue to use, ManageEngine ServiceDesk Plus software to track and route incidents, send email notifications, and provide notice on software updates and resolution of reported issues. ServiceDesk Plus provides SIROMS Helpdesk with the functionality to be an exceedingly responsive resource that benefits SIROMS end-users by maintaining focus on their mission—assisting State residents impacted by Superstorm Sandy, COVID-19 and Hurricane IDA.

Helpdesk technicians, and select DCA staff, may access this web-based portal to capture all incidents reported via email and phone call. ServiceDesk Plus provides a centralized repository to manage and track end user, development, and implementation service requests. It also allows the Helpdesk to track incidents and events, as well as manage the priority, status, scheduling, and resolution of service requests.

SERVICEDESK PLUS CAPABILITIES

ServiceDesk Plus provides the following capabilities:

- View the summary of current requests
- Submit online incident tickets
- View status of tickets and solutions to common issues
- Change ticket status (e.g., on hold, pending customer action) when additional information is needed for Helpdesk to troubleshoot and resolve the issue.
- View status and history of incidents
- Send requestor notifications regarding opening and closing of tickets

- Customizable reporting to measure performance across a broad spectrum of requests, incidents, changes, and surveys. Includes parameters such as Priority, Department, Technician, Requester, Assigned Technician, start times/closing times, and request types (by Category, Subcategory, Priority, etc.).

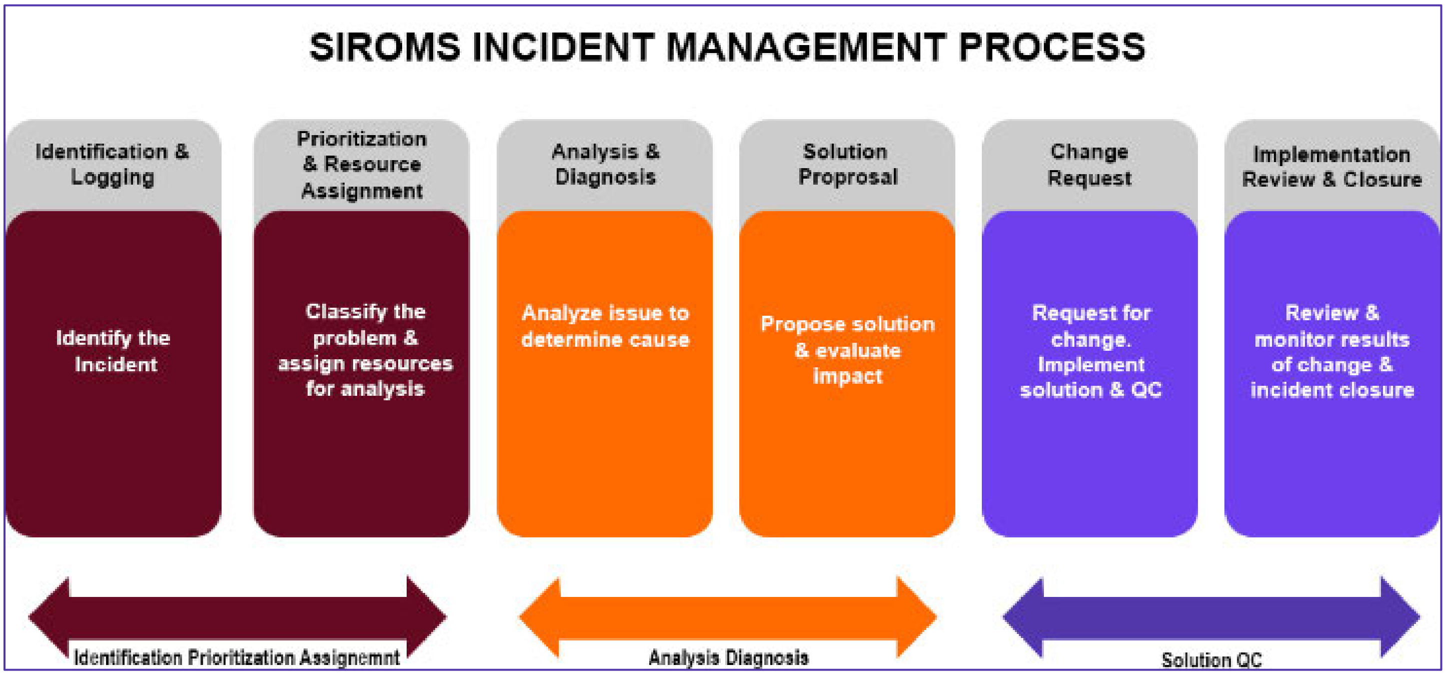
HELPDESK TICKET INTAKE

The SIROMS Helpdesk is available via a number of communication methods including email, phone, or online web submission. Helpdesk requests are primarily accepted via email at Helpdesk@SIROMS.com. Phone requests will be accepted via a DCA-DRM assigned phone number. Online web submissions are available to select DCA-DRM staff.

SIROMS INCIDENT MANAGEMENT PROCESS

When tickets are submitted, Helpdesk will follow the incident management process below to help ensure that user concerns are documented, evaluated, appropriately resolved and responded to. If report or software changes are needed, they will be documented and scheduled in coordination with DCA-DRM based on prioritization.

Exhibit 8 - SIROMS Incident Management Process


SIROMS INCIDENT MANAGEMENT PROCESS
Identification & Logging
Identify the Incident
Prioritization & Resource Assignment
Classify the problem & assign resources for analysis
Analysis & Diagnosis
Analyze issue to determine cause
Solution Proprosal
Propose solution & evaluate impact
Change Request
Request for change. Implement solution & QC
Implementation Review & Closure
Review & monitor results of change & incident closure
Identification Prioritization Assignemnt
Analysis Diagnosis
Solution QC

INCIDENT IDENTIFICATION AND LOGGING

When a user communicates to Helpdesk, they are typically seeking a response to a question, requesting a system or report change, or requesting that a system or report issue be resolved. Upon receipt of the communication from a user, the Helpdesk will log the communication in the form of a ticket. This will trigger an email to the user confirming receipt of their communication.

PRIORITIZATION AND RESOURCE ASSIGNMENT

In addition to the details of the reported incident, the SIROMS Helpdesk categorizes the request based on the incident prioritization (Critical, High, Medium, and Low), service type required (Functional or Technical), and the affected SIROMS modules. Additional communication with the user may be required to help ensure tickets are properly categorized.

Requests are categorized or grouped using the following attributes: **Service Category**, **Category**, and **Sub-categories**. A request to move an application to the next stage can be put under the request **Service Category:** *Software*, **Category**: *Ida*, and **Sub-Category:** *HARP*. Similarly, if there is a problem in the way an application is functioning, it can be categorized under the **Service Category**: *Software*, **Category**: *Software Maintenance Request*, and **Sub-Category**: *CIM*.

The SIROMS Helpdesk has created numerous service categories, categories, and sub-categories for the SIROMS project. These service categories, categories, and sub-categories will be listed under the respective drop-down menus available in all new requests and will be used to help enhance the metrics, organization, and reporting required. These further improve the ability to provide statistical information and identify trends, which allows the Helpdesk to alert the project team when there are multiple tickets regarding the same issue. These categories also enhance our ability to build reports that display a variety of metrics.

ANALYSIS AND DIAGNOSIS

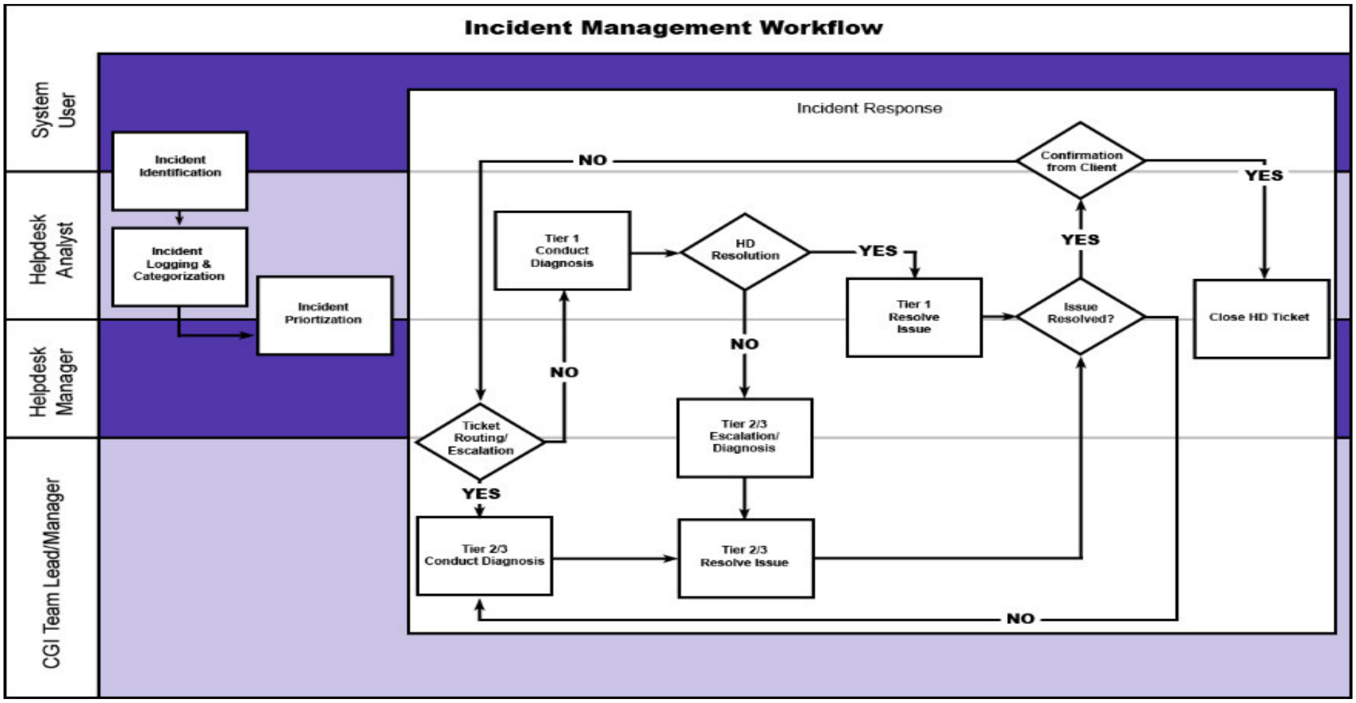
Once an incident has been recorded, incident investigation and analysis begin. A SIROMS Helpdesk technician will troubleshoot, test, and check possible scenarios to come to a resolution. If a resolution cannot be reached by Tier 1 staff, it is then escalated and assigned to the next Tier. The SIROMS Helpdesk continues to maintain communication with all Tiers to coordinate the tasks required and provide feedback to the end user.

The Tiers are described as follows:

- 1st Level/Tier support provided by the SIROMS Helpdesk to triage incoming issues, determine severity, route ticket(s) accordingly, and follow-up as necessary.
- 2nd Level/Tier support to diagnose if the request is a defect, user training/configuration issue, or if there is a potential need for a system enhancement (Change Request).
- 3rd Level/Tier support to provide final diagnosis and resolution path with cross functional teams including business, database, application, reporting, network, and infrastructure.

The SIROMS incident management workflow, which conforms to the ITIL standards, is demonstrated in Exhibit 9 below.

Exhibit 9 – Incident Management Workflow



In the event the Helpdesk technician has exhausted all attempts to resolve the incident, the incident will be escalated accordingly until a resolution is determined. The escalation and assignment of a particular incident is dependent on the nature of issue, complexity of issue, and whether all pertinent information has been given to the CGI team to allow proper troubleshooting. Escalated incidents are typically sent to the Business Analysts to assist with the diagnosis. The Business Analyst will either provide a resolution, potentially after communicating with the user, or identify that the issue needs to be reassigned to system development, report development or database. At that point, the Business Analyst will remain involved in the incident, providing functional expertise, as needed, until a viable solution is identified. All incidents escalated beyond Tier 1 will have regular follow-ups documented in addition to system user updates. During the time spent troubleshooting and resolving the incident, Helpdesk follows up on aging tickets and provides status updates in the notes and resolution section of the ticket. Any aging tickets are routed to managers for immediate escalation.

SOLUTION PROPOSAL

Once a solution is identified either by the Business Analyst or the technical team, it will be communicated back to the user via the Helpdesk or the assigned Business Analyst. The solution may simply be to provide user guidance on how to perform a certain task, it may be confirmation that their request has been implemented, or it may require more elaborate discussions regarding different options to resolve the problem. For less complex solutions, upon successful resolution of the incident, a technician will communicate appropriate instructions to verify that the incident has been resolved to the end-user who reported the incident.

CHANGE REQUEST

In the event a software or a report fix may be needed, the SIROMS Helpdesk will facilitate discussions with the appropriate Business Analyst and Technical Resource. In these instances, root cause analysis will be completed, if necessary, and solutions and their impacts will be documented and provided to the user and the DCA-DRM PMO to determine the path forward. Depending on the severity and priority, that may include an off-cycle deployment, re-prioritization of existing CRs to implement the change in the current scheduled release, or the scheduling of an official change request for a future release.

Off-cycle deployments will be made to resolve high-priority, high-impact issues. These fixes will be thoroughly tested by the CGI QC team before being sent back to the user and/or DCA-DRM PMO for confirmation. Once approved by DCA-DRM, they will be implemented as soon as practicable.

In the event a helpdesk ticket results in the need for a change request, that will be discussed with the DCA-DRM PMO and a change request will be logged in the system (see section 2.2.6). The change request will be targeted for a scheduled release and the helpdesk ticket will be closed.

IMPLEMENTATION REVIEW AND CLOSURE

Once the client has verified the solution, the incident will be closed. A follow-up email will be sent to the client for resolution confirmation. Helpdesk will also confirm that the initial classification details are accurate for future reference and reporting. The SIROMS Helpdesk maintains a complete history of records for all incidents reported. Relevant details that are tracked include, date/time stamping, user information, descriptions, related tickets and incident resolution details.

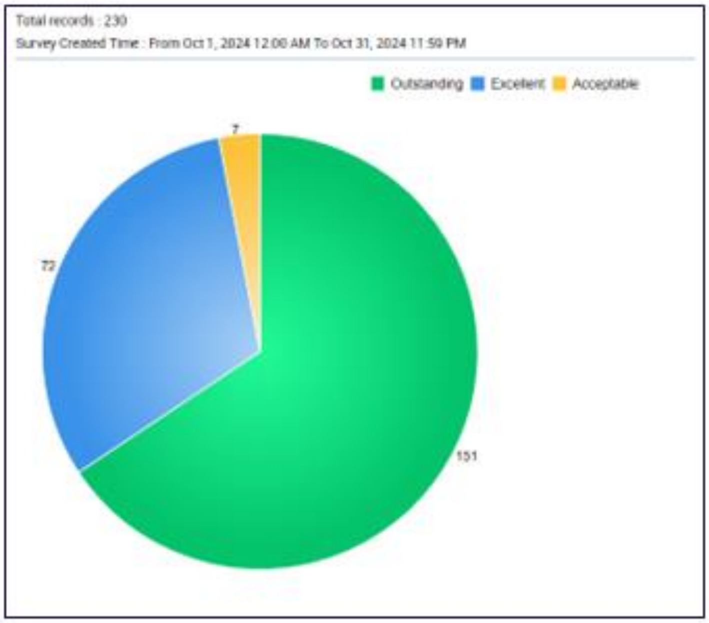
END USER SURVEY

After completion/closure of incident, a link to our End User Satisfaction Survey is sent out to determine overall satisfaction with the helpdesk service delivery. SIROMS uses a number of best practices to formulate the user satisfaction survey including but not limited to:

- Explain the purpose of the survey
- Easy to use rating system
- End user comment section

The results of this survey can be compiled and provided to DCA quarterly or upon SCM request. Exhibit 10 below depicts the End User Satisfaction Survey results for October 2024. CGI understands that DCA-DRM also requires reporting and access into service level data to confirm that minimally, 95% of tickets are being responded to within 24 hours. We will work with DCA to determine the details and frequency of the information to be provided upon contract award.

Exhibit 10 - End User Survey Results Report



SIROMS SYSTEM INTERRUPTION AND ESCALATION PROCEDURES PLAN

The SIROMS technical team has tracking measures in place to actively monitor both known and unknown issues that may negatively impact system performance over the course of the project. In the instance of a service interruption, the SIROMS System Interruption and Escalation Procedures Plan provides the overall guidance for CGI actions/processes, communication, and identifies key roles/personnel during an unplanned system service interruption. This plan will be triggered by any reported service interruption and will be in effect until SIROMS system performance is restored to full capacity.

Notifications

CGI considers any unplanned service interruption or event affecting the System’s functionality as a critical incident. An incident ticket in ServiceDesk Plus will document the issue the user is experiencing, record which user reported the incident, and log the time and current status of the service interruption. Once the ticket is logged, an internal notification will be sent to the CGI Team to assess the issue reported and confirm a service interruption. Upon confirmation, a notification will be sent to DCA-DRM SCM within 30 minutes to notify of a service interruption and provide any known details regarding the issue, and updates will be provided every 2 hours. Additionally, an email communication to SIROMS system users will be sent to notify DCA-DRM SIROMS staff and end users of the system interruption. Once the issue is resolved and the system is functioning as normal, an email will be sent notifying the DCA-DRM SCM and all SIROMS end users. Each notification will be sent via the ServiceDesk Plus ticket or mass email notification, including service interruption status updates, and resolution.

Incident Ticket Tracking

Due to the complexities with the SIROMS technical architecture and functional programming, an incident may require multiple CGI resources to investigate the true nature of an issue's cause. In logging the initial incident, the SIROMS Helpdesk will open a ticket that will function as the "parent" incident ticket. Subsequent tickets will be created for teams (Functional, Development, Infrastructure, and Reporting) to track related work associated with identifying the cause and resolution; these will be linked to the 'parent' ticket. This process identifies related tickets to help ensure accountability that all required analysis is completed, logged, and referenced in the event a similar incident is recorded in the future. The parent ticket will be disclosed to the SCM for reference.

Key Roles and Responsibilities

During a service interruption, timely and factual communication is essential to the effort of returning SIROMS back to full capacity. CGI recognizes that it is a collaborative effort in returning the system back to normal and identifies key roles and responsibilities for both DCA-DRM and CGI below.

DCA-DRM SCM (State Contract Manager)

- The DCA-DRM SCM acts as the first point of contact for CGI to report a service interruption and confirmation within 30 minutes.
- DCA-DRM SCM is responsible for approving any necessary actions or emergency system changes related to the unplanned service interruption.
- In the event that the DCA-DRM SCM is unavailable, CGI will notify the designated replacement.

CGI Project Manager

- The CGI Project Manager acts as the first point of contact for information regarding the service interruption and will provide the DCA-DRM SCM with known details as they are validated and confirmed.
- The CGI Project Manager may designate a communication lead for a service interruption and share the responsibility of communication regarding updates with the SIROMS Helpdesk Manager.

Helpdesk Manager

- Creates and updates the incident ticket and is responsible for coordinating communication to system users within 30 minutes after verification of a service interruption.
- Verifies the service interruption and updates CGI team members required to assist in resolving the incident.
- Opens the parent incident ticket and links all related incident tickets to the parent.
- Communicates ticket information to all relevant CGI team members.
- Provides ongoing communication every two hours until the issue is resolved.

Programmer/Technical Lead/Incident Coordinator:

- Communicates updates to relevant teams regarding progress and when resolution has been found.

HOURS OF SERVICE

Standard hours of operation are from 8:00am to 5:00pm, Monday through Friday during all state workdays.

PRODUCTION SUPPORT/STAFFING

Staffing for the SIROMS Helpdesk is based on the service levels and the amount of user support anticipated for the project. Examples of support would include:

- Inbound calls and emails for Tier 1 Support
- Escalation and response for Tier 2 and Tier 3 support including:
  - Support for defects
  - Training
  - Documentation
  - Usability of systems or reports

CGI plans for Helpdesk scalability during service interruptions as well as planned system updates and maintenance. For short-term increases in ticket volume, such as during service interruptions or planned system updates and maintenance, we leverage the support of our functional Subject Matter Experts, all of whom have received training in Helpdesk operations. However, in the case of sustained volume increases, we will require the augmentation of our Helpdesk team through the addition of new staff. Longer term Helpdesk needs will be addressed in accordance with our established staffing procedures documented in section 2.3.2.

HELPDESK SERVICE LEVEL AGREEMENT (SLA)

CGI understands a timely response to all reported user requests to the Help Desk is essential to supporting a fully functional SIROMS user community. Help Desk strives to create and respond to user requests within 24 hours; we anticipate that we will meet or exceed the 95% required by DCA-DRM. The response may be a resolution to the issue or an escalation of the issue to the development team for further evaluation and resolution.

The ability for the SIROMS Helpdesk to provide quick turnaround for access requests has many elements outside of CGI control. Provisioning for general User Access, Reporting, Development, Database, Software, and Maintenance requests will vary as they are dependent on:

- Time of request submission
- Approvals from DCA-DRM management
- Client verifications

TRAINING

Given the quickly evolving nature of SIROMS, CGI recognizes the need for Helpdesk to stay abreast of new and changing functionality and associated reports. To help ensure knowledge transfer, Helpdesk staff participate in a number of system change related sessions:

- Internal walkthroughs of Business Functional Requirements Documents (BFRDs), where Business Analysts review change requests and associated business needs in detail and discuss implementation with the technical teams

- Weekly cross-functional meetings where helpdesk tickets and change requests status are discussed as well as any outstanding questions or issues
- Internal reviews of user testing materials before delivery to DCA-DRM

Helpdesk also has access to:

- BFRDs
- User permissions summaries
- Module workflows
- The test environment to run scenarios and test issues
- CGI SMEs to field questions when needed

DOCUMENTATION

Helpdesk creates, updates, and maintains documentation pertaining to all relevant functions including, but not limited to:

- **Incident management** - ServiceDesk maintains a comprehensive record of the entire incident process flow, from creation to resolution, by documenting the different statuses, assigned technicians working to resolve the incident, and both external and internal communication needed to resolve the incident experienced by DCA-DRM or end users.
- **End user support** - ServiceDesk contains all communication, including email chains and phone call logs, that occur with the end user. This allows Helpdesk to document and track exactly what the user is experiencing to better assist in resolving their incident in an efficient manner. Helpdesk also documents the end user's confirmation of resolution in the ticket to help ensure closure of the ticket is valid.
- **Security** - ServiceDesk logs a private record of usernames and passwords to assist end users when a new account is created, or they are having difficulties accessing their SIROMS BPM accounts. Helpdesk also receives notice of accounts approaching inactivity, password updates by the users, and when accounts are locked or disabled.
- **Application support** - Through ServiceDesk, categorization of tickets by the affected module(s) is possible. This allows for CGI to better recreate the user's issue and customize fixes to help ensure that solutions are reached. It also assists Helpdesk in tracking which modules more or less frequently have incidents logged to alert the CGI team to a potential longer-term solution maybe being necessary.
- **Escalation support** - ServiceDesk keeps a comprehensive record of the Tiers that a ticket gets escalated to and which technicians are responsible for investigating or implementing a fix to resolve an incident. Internal communication is tracked to help ensure that all records are maintained for both CGI and DCA-DRM use if necessary. It also allows for a quicker solution to be reached if a similar incident resurfaces as the steps to the initial resolution were documented.
- **Organizational charts** - Helpdesk possesses lists of both DCA-DRM and CGI team members that are responsible for the different SIROMS modules. This allows the process of request approvals (external) and ticket escalation (internal) to be seamlessly tracked and executed to help ensure incidents are resolved as efficiently as possible.

2.2.4 System Administration

CGI has hosted and managed the technical and application infrastructure for SIROMS for the past ten years in CGI’s private cloud and will completely migrate the SIROMS SaaS solution to the AWS government cloud. This environment will be leveraged to deliver SIROMS through public URLs via browsers and mobile devices. CGI has increased the stability of SIROMS yearly to achieve industry standards for uptime. We have acquired a wealth of experience in SIROMS operations and developed numerous tools and health checks to proactively monitor the current SIROMS infrastructure. CGI has also worked with DCA-DRM to consolidate or expand hardware needs based on changes in the number of SIROMS users. For consolidation and expansion of hardware based on changing demand, CGI's deep expertise in the SIROMS platform is crucial in to keep SIROMS functional with optimal cost and efficiency. While the section below contains an overview of these details, the Infrastructure Overview document can be found in Appendix E.

CGI recognizes DCA-DRM's needs in establishing and maintaining the software that is essential to meeting their disaster recovery commitments. When new legislation is passed and new programs are launched, DCA-DRM looks to fulfill the needs of New Jersey citizens as quickly as possible to disburse funds in an accurate manner that meets federal reporting requirements. CGI collaborates closely with DCA-DRM to identify any new hardware needs as quickly as possible to help ensure there are no bottlenecks to achieving their mission.

Before rolling out application or report changes to system users, verification that the changes match the requirements and function correctly is necessary to avoid any negative impact on the production environment. To provide the State with a testing environment that allows for this verification to be done as thoroughly and rapidly as possible, CGI refreshes the environment with production data on a monthly basis. Scheduling these refreshes requires careful coordination with DCA-DRM. CGI works closely with DCA-DRM to determine the optimal time between user testing, demonstrations, trainings, and any other needs that the state has to avoid an outage or an unexpected change in data at a time when the test environment needs to be available.

CGI has designed processes that allow the reporting databases to be refreshed daily using nightly ETL jobs that bring the reporting database in sync with the application database, within 24 hours. Reports are generated using data from the reporting database.

Failure to appropriately maintain the system hardware, software, and test data increases the risk of not being able to deliver disaster recovery services to citizens of New Jersey. CGI will leverage its decade of experience in delivering these services to continue to help DCA-DRM achieve its goals.

There are several points of clarification we would like to make.

- Since CGI via AWS is hosting the PaaS environment, DCA-DRM is renting the infrastructure from CGI and not actually purchasing it. Consequently, at the end of the contract no physical infrastructure can be turned over to the State.
- CGI expects no additional hardware devices, not hosted within the PaaS, to be purchased by the State in conjunction with SIROMS.
- State-owned software licenses will be removed from all CGI managed servers. CGI will investigate options for transferring licenses that were purchased through CGI on the State's behalf. However, licenses that are part of the overall infrastructure, such as operating systems and SQL Server are non-transferrable and are considered a managed services license that is integrated into the hosting charge.
- As indicated in the Infrastructure Overview document (see Appendix E), CGI maintains several different environments for the SIROMS project including Production, Disaster Recovery, UAT,

and Development. No separate reporting environment exists, however reporting databases exist within each of the aforementioned environments.

- To save cost for the State, the SIROMS Development environment is not located within a NIST 800-53 rev 5 level hosting facility and consequently only obfuscated production data can be used in the Development environment.
- The UAT environment is refreshed from production on an as needed basis depending upon the type of change requests that are being tested. CGI is prepared to refresh the data in the UAT environment on a monthly basis, but the timing of the refreshes needs to be chosen carefully each month. The timing needs to take into account, any system or report testing that is currently in progress and refreshes should be avoided the week after a production deployment to help ensure a stable UAT environment is available after a production release.
- Files will be stored using Opentext's Enterprise Content Management (ECM) software to help ensure that the files are stored in a secure manner that allows them to be easily accessed by authorized system users.

2.2.5 Data Warehouse Environment

The SIROMS data warehouse, at its core, is built on MS SQL Server using SQL Server Integration Services for ETL and SQL Data replication for real time data. The data warehouse simplifies and speeds up data retrieval by using the concept of Business Process Views. The process views are similar to the OLAP (Online Analytical Processing) data models, which makes it easier to report on a large volume of data. The following components help in building and maintaining the data warehouse:

- **SQL Server Integration Services ETL** - SQL Server Integration Services (SSIS) is a powerful ETL tool, which is included with the MS SQL Server Enterprise Edition License. The capabilities of the tool range from building simple ETLs, using drag and drop to build powerful transformations using PLSQL, .NET, or other modern scripting languages. The ETL helps to intake data from external or internal systems and transforms the datasets to build a data repository, tailored for reporting needs. The data is de-normalized to facilitate better support for reporting queries and increased performance. In addition to the intake of data, SSIS also has the ability to send data out to external systems. Notification emails for acknowledgements are also generated to keep the user acknowledged and informed of the status of the upload. ETL helps keep the data warehouse current with information from both external and internal systems, which provide critical data, needed for SIROMS Reports.
- **SQL Server Replication –** SQL server replication is a powerful way of extracting real time data for reporting needs. Replication allows the Online Transaction Processing (OLTP) system to free up resources, needed for the front-end applications, while allowing the data warehouse to use real time data. Replication, along with ETL helps in keeping the data warehouse in sync with the OLTP as well as the external systems.
- **SIROMS Integration Engine –** The SIROMS Integration engine, built by CGI, is a proven and trusted approach to transfer data needed for the data warehouse. The ability to create inbound and outbound interfaces to complex systems makes it a critical component. The integration engine allows the users to drop files through FTP or SharePoint to leverage the ETL intake process. Data related to interface transfers are also captured in the data warehouse.
- **MS SQL Server Agent** - The SQL Server Agent is a tool used in scheduling ETLs and SQL jobs, required to maintain and refresh the SIROMS data warehouse. The SQL Server Agent helps in

refreshing the data warehouse based on a specified job frequency. Typically, all the tables in the data warehouse are refreshed from the OLTP on a daily basis.

- **Data Warehouse Security** – The data warehouse is hosted in firewall controlled FedRAMP moderate environment with users requiring 2 factor authentication. The end users of the system will not have direct access to the data warehouse environment. The authorization of users, who have access through 2 factor authentication is controlled using a combination of database roles and windows access controls. Data dumps for specific tables, can be generated for selected third parties, as directed by SCM.

The Business Intelligence and Data analytics solution, built on the foundation of a centralized and robust data warehouse, serves the reporting and analytics needs with reliability and precision The Business Intelligence and analytics suite consists of Microsoft SQL Server Reporting services for paginated and operational reports, Tableau and d3 for visualization and analytics. The Business Intelligence and analytics solution empowers clients to be data driven decision makers at various levels including day to day operations to support to strategic objectives.

SIROMS Reporting Environment Features:

- CGI utilizes the capabilities of Microsoft Business intelligence tools and Tableau platform to create and deliver a large volume of reports.
- CGI uses SQL Server Report Builder as a metadata layer to generate the reports. The SQL Server Report Builder simplifies the data model, making it reusable and modular.
- The reports can be saved and exported to Excel, PDF, Word, XML or CSV formats.
- The reports are scheduled to the approved end users in Excel or PDF formats. Scheduled reports are delivered via email to the end users' inboxes and if required can be delivered to SharePoint or other collaboration platforms. Tableau dashboards can be emailed with a pdf or image embedded in the email, which allows the users to click and view the dashboard if they have the right privileges.
- Some of the reports use dynamic reporting framework that would adapt to changes in the application. The dynamic approach helps in improving the time needed to roll out new features to users in an accelerated fashion eliminating the need to modify the report for every application change.
- Users have the option to request certain reports from the SIROMS application pages. The SIROMS BPM application is integrated with SSRS report engine. The users can click a button in the application page to have the report delivered to their email.
- At a high level the following types of report are created from the system:
  - **Ad-hoc Reports –** Since the beginning of SIROMS in 2013 CGI delivered close to 4500 ad-hoc reports. CGI maintains frequently requested ad-hoc queries as separate reporting templates so that the queries can be reused if needed. The volume of ad-hoc report requests increases significantly during the audit process and CGI has consistently demonstrated the ability to respond to ad-hoc requests within the timeframe requested.
  - **Canned Reports:**

      - **Executive Level Dashboards** – CGI has built numerous dashboards, which have helped in providing program summaries and areas of concern to executive management. These dashboards are created at various levels to help ensure that all of the metrics needed are captured. The executive dashboards include all of the financial and operational metrics needed to track the progress of the particular program.

- **Operational Support Reports –** Operational reports, which show the operational status of each application or a financial transaction, helps provide data needed for the day-to-day activities of the end users.
- **Audit Reports**- These reports include data needed to support quarterly audits by HUD and help to gather information from partners agencies.
- **System Assurance Reports** - System assurance reports include data related to interface transfers or any other data needed to help ensure the data integrity of the system.
- **ESRI Reporting** - ESRI, a global leader in Geographic Information System (GIS) technology, offers a comprehensive suite of reporting capabilities through its ArcGIS platform. The reporting solutions are designed to provide insightful, actionable, and data-driven results that meet the diverse needs of organizations. It can provide various type of reporting needs such as Mapping reports, Spatial Analysis Reports, Statistical Reports, Trend Analysis, Operation Reports. Demographics Reports and Custom-Tailored reports. ESRI's ArcGIS platform integrates with our applications and databases, enabling the generation of both standard and highly specialized reports. Our reporting capabilities are designed to provide clarity, support decision-making, and enhance strategic planning across various sectors and can be tailored based on requirements.
- **Statewide Mitigation Data Collection and Reporting** – Statewide Mitigation is an effort that integrates various SIROMS and external data sources and provides the ability to create a consolidated report in identifying duplication of benefits information and perform data analysis. The data collected from multiple sources are maintained in a separate database using data warehousing best practices such as performing Data Cleansing, Refinement, ETL and refreshing regularly and checking the data integrity as it fits. PII information is also removed and retracted where necessary during the process. The overall consolidated data can provide various reporting options and Key Performance Indicators (KPIs). This can become a valuable input for making informed business decisions and provide data feeds for various transparency websites as well.

2.2.6 Technical Services

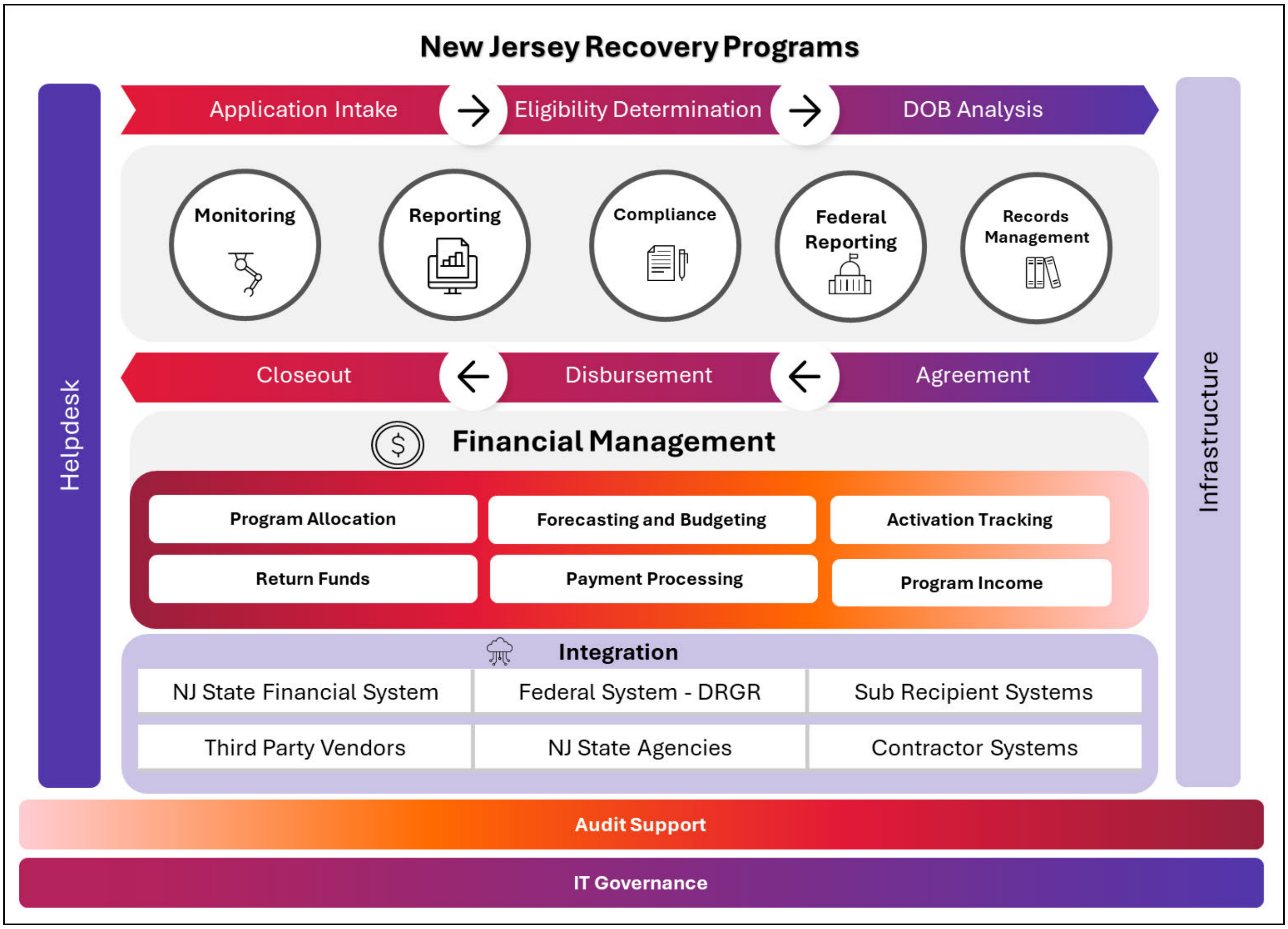
Based on our years of expertise, developed by working closely with the State of New Jersey, CGI will provide a team with the capabilities needed to maintain SIROMS. The team is experienced in designing, developing, testing, and supporting software, specifically for disaster recovery program management for DCA-DRM. This understanding of disaster recovery program management, at all phases of the software development life cycle, provides additional verification at every step to help ensure that changes are being developed consistent with the needs of the project.

The business analysts on the team have a deep knowledge of the goals of the individual programs and the federal requirements that need to be met while achieving these goals. They continuously leverage this knowledge first to work closely with state program and finance representatives to suggest ways in which the SIROMS solution can be employed to solve the State's challenges and design the system functionality that meets program requirements while remaining compliant with governmental financial requirements.

During the process of supporting DCA-DRM’s disaster recovery objectives, CGI assessed New Jersey’s disaster recovery program, along with any legacy information and record keeping systems and provided an action plan targeted to provide rapid deployment of the CDBG-DR Programs to assist State residents impacted by Superstorm Sandy. Features developed by CGI to support these objectives include:

- Comprehensive Financial Management system with ability to link to State Treasury systems, banks, and applications for electronic funds disbursement
- Financial Management capability to manage disparate funding sources, allowing the primary Grant recipient to combine data for holistic recovery reporting, while maintaining the ability to track, manage, and report on each funding source results individually
- Multiple Full Life Cycle Grants Management systems that include public facing application intake systems, application randomization, eligibility determination and scoring, at-a-glance workflow status, document repository (record retention), complex grant award calculations, system generated grant award agreements, status and history tracking to provide clear audit trail of all actions taken within the system, and direct integration with the State treasury for funds disbursement
- Integration with major federal grant management systems to support federal and programmatic reporting requirements
- Program administration and policy information support
- An integrated data warehouse containing consolidated data provided by all partner agency sub-grantees driving multiple transparency portals including the Governor’s Office of Recovery and Rebuilding (GORR) and the Office of the Comptroller
- Statistical analysis and forecasting methodologies which have helped the State identify bottlenecks in operations, provide estimates on program completion, plan for resource allocations, and project the rate of grant disbursements through the life of the programs

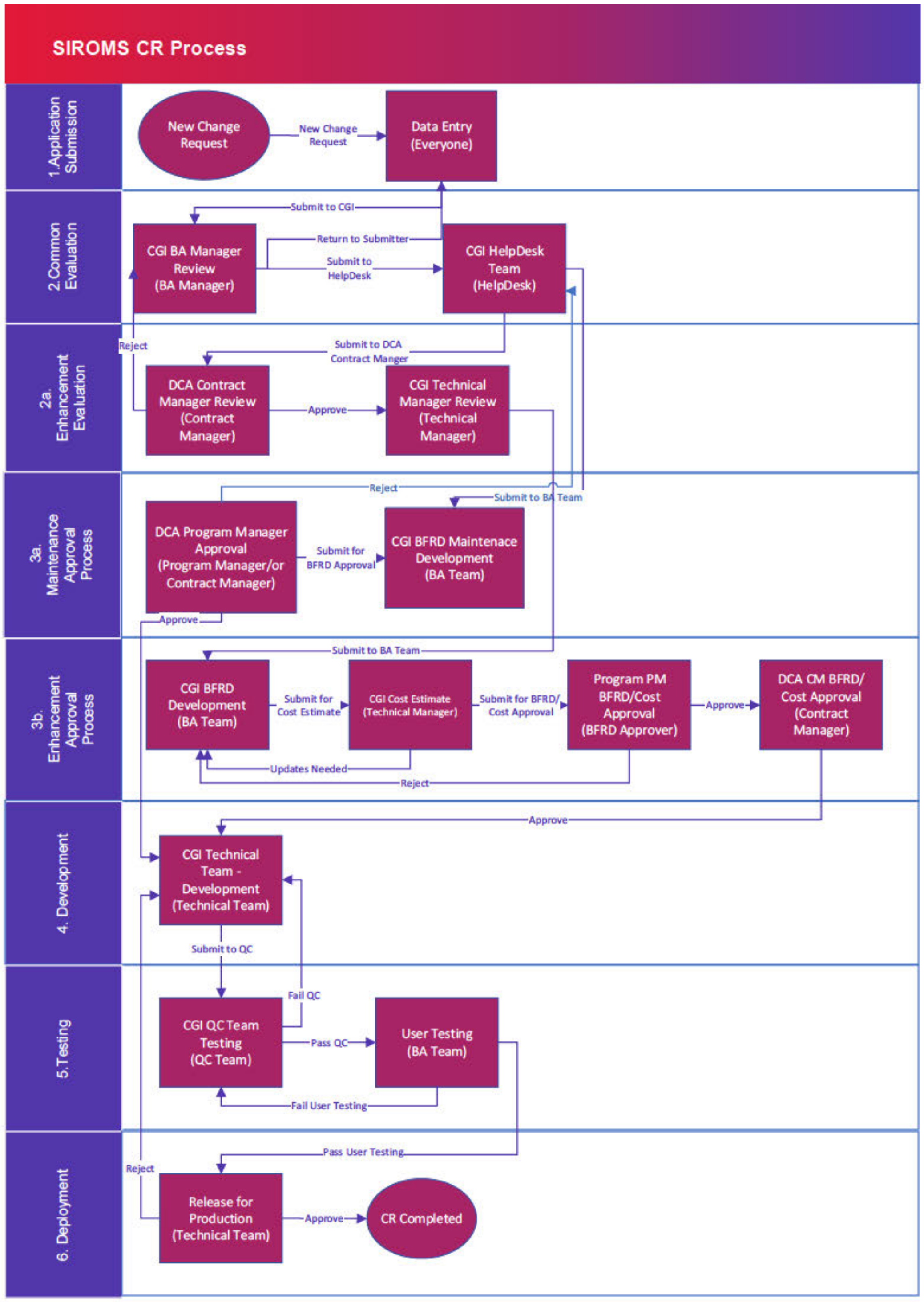
Exhibit 11 - SIROMS Functional Overview



System Change Request Process

CGI utilizes the System Change Request module that is built into SIROMS for the purposes of tracking potential challenges that SIROMS may be modified to solve. This module allows the SCM to track the progress of every proposed change through the System Change Request process and to approve or reject the change at multiple points in the process. The SCM can have the change request put on hold, to temporarily prevent any further work from being done on it while further review is done, or withdraw the change to permanently prevent further work from being done. The image below shows the life cycle of a System Change Request from creation to release for production. Note that maintenance change requests require approval by the state program manager and enhancement change requests require approval by the state program manager and the SCM.

Exhibit 12 – SIROMS System Change Request Process


SIROMS CR Process
1.Application Submission
2.Common Evaluation
2a. Enhancement Evaluation
3a. Maintenance Approval Process
3b. Enhancement Approval Process
4. Development
5.Testing
6. Deployment
New Change Request
New Change Request
Data Entry (Everyone)
Submit to CGI
Return to Submitter
CGI BA Manager Review (BA Manager)
Submit to HelpDesk
CGI HelpDesk Team (HelpDesk)
Reject
Submit to DCA Contract Manger
DCA Contract Manager Review (Contract Manager)
Approve
CGI Technical Manager Review (Technical Manager)
Reject
Submit to BA Team
DCA Program Manager Approval (Program Manager/or Contract Manager)
Submit for BFRD Approval
CGI BFRD Maintenace Development (BA Team)
Approve
Submit to BA Team
CGI BFRD Development (BA Team)
Submit for Cost Estimate
CGI Cost Estimate (Technical Manager)
Submit for BFRD/ Cost Approval
Program PM BFRD/Cost Approval (BFRD Approver)
Approve
DCA CM BFRD/ Cost Approval (Contract Manager)
Updates Needed
Reject
Approve
CGI Technical Team - Development (Technical Team)
Submit to QC
Fail QC
CGI QC Team Testing (QC Team)
Pass QC
User Testing (BA Team)
Fail User Testing
Pass User Testing
Reject
Release for Production (Technical Team)
Approve
CR Completed

The table below shows information tracked with every System Change Request and its relevance to the SCM.

Exhibit 13 - Change Request Components

Field	Description
Reason For Change	The description of the problem to be addressed by the change request
Description of Change	Detailed description of the change proposed to solve the problem
Production Estimated Release Date	The date the change is intended to be promoted to production. This field is used to prioritize and schedule the changes
Complexity Cost Range	A rough estimate of the cost required to complete the change. This field can be used early in the life cycle to determine if the change is worth the effort involved
Cost Estimate	The actual estimated cost. This is provided after the BFRD has been approved and supports DCA's ability to view anticipated costs at the CR level.
Document Attachments	This can be used to attach multiple files to the change request. All versions of the BFRD should be attached to the change request

CGI recognizes that there may be stand-alone initiatives that require the need to be managed separately, the Mobile Inspection Application or AWS Server Migration are recent examples. In these instances, the process of using the Change Request tool would still be used, but additional project management activities may be employed. CGI will work with DCA to determine the best approach for managing these types of projects but anticipates the need to leverage a Microsoft Project Plan to detail key tasks, timelines and resources. This will not only serve to set realistic expectations of the implementation but will help identify staffing needs and estimated overall costs.

BUSINESS AND FUNCTIONAL REQUIREMENTS DOCUMENTATION

CGI business analysts will analyze each Change Request (CR) and facilitate Joint Application Design (JAD) sessions with appropriate DCA-DRM stakeholders to elicit change prerequisites and conditions. Through these JAD sessions, CR requirements are derived to form a Business/Functional Requirements Document (BFRD). Business analysts will continue to revise content within each BFRD until it is finalized. DCA-DRM is required to approve the finalized BFRD before development can begin. Finalized BFRDs are posted to the associated SIROMS Change Request for approval to proceed with development.

Please see section 2.2.8 for more details on the requirement management process.

DEVELOPMENT & QUALITY CONTROL

The detailed requirements in approved BFRDs are used by the development and Quality Control (QC) teams as the basis for system/reporting development and QC script development. Business analysts will review scripts to confirm functional and technical requirements will be met and provide feedback to developers and QC analysts to finalize the script.

Quality control analysts will perform testing on each scenario defined in the script within the testing environment. Issues that are found during QC will be reported to developers, who will respond to QC in a timely manner with a resolution on each issue. Business analysts will support the QC and development teams as needed to prioritize resolution of issues and prepare each CR for User Acceptance Testing (UAT) sessions.

USER ACCEPTANCE

User Acceptance Testing (UAT) is a shared responsibility of both the DCA-DRM and CGI teams. UAT is a formal testing effort administered by CGI and completed by DCA-DRM program users to determine whether new or updated system changes adhere to the business requirements as specified in the BFRD. Diligent testing and reporting of issues found during UAT is essential since program users will possess detailed knowledge of the program needs that may not necessarily be replicated in unit or system testing efforts. UAT testers validate software releases and provide the necessary feedback for the SCM and the CGI Team to either approve/deny the production release. CGI will intake issues reported for the purpose of documenting, tracking, and resolution.

CGI will administer hands-on UAT sessions, augmented with a testing checklist of any new or updated software components developed as requested by DCA-DRM SCM or program users. Five days will be provided for UAT of any system, database, or report release assuming that there were no adjustments to the defined release schedule or delays in obtaining BFRD approvals and that design changes/updates were minimal after approval. The UAT sessions will be administered within a UAT environment that contains user accounts that mirror production level access including data that has been refreshed in the last 30 days. CGI will work closely with the SCM to adhere to the scheduled outline as the normal course of action. In the instance that the scheduled outline deviates from normal, as a result of competing priorities, priority business needs, or production issues, CGI will discuss with the SCM an appropriate course of action to these one-off cases.

Any defects, bugs, or design revisions found in UAT will be measured against the approved BFRD and prioritized for resolution. Once code revisions are available for testing, the new code will undergo system testing and regression testing efforts prior to promotion to UAT. Code promoted to production will be free of known critical errors or otherwise approved by the SCM for promotion to production. Non-critical issues which will not be resolved by the scheduled release date will be evaluated and queued for a future release date.

USER ACCEPTANCE TESTING MATERIALS

User acceptance testing is a fundamental aspect to helping ensure that requirements agreed upon by the State and CGI are met prior to production implementation. Unless otherwise agreed to by CGI and the SCM, CGI will hold user acceptance testing sessions to present system changes. During these sessions, users will be provided with presentation materials that will be leveraged to train on the new or modified functionality associated with the change request. Copies of these materials will be provided to the users for future reference.

Additionally, users will be provided a checklist of all the essential requirements associated with the change request. For each requirement, participating users will be required to indicate whether the requirement was met. Any requirement that has not been met will be prioritized and addressed.

Completed checklists must be received within three (3) business days of the production release and will provide the basis for determining if the associated change is approved for release. Completed checklists from participating users as well as the presentation materials will be posted to the change request folder in BPM.

IMPLEMENTATION

Once user acceptance testing is successfully completed and approved by DCA-DRM, implementation is the final step in the process to integrate a newly approved and accepted change into the production environment. The implementation method itself will include a systematic structured series of steps which mimic the steps previously taken to integrate a new or enhanced change through testing and UAT environments. The new or enhanced change will be certified for use in production once all implementation steps have been completed.

As part of the implementation process, the CGI Team will be responsible for providing training, documentation, and support to DCA-DRM staff on new or enhanced software or hardware components. CGI will develop and provide a summary of each CR released to production, will work with DCA-DRM to facilitate the assignment of user roles to system users, and post to a DCA-DRM repository requested documentation such as workflows and user permissions.

TRAINING

Training is a key component to enabling DCA-DRM program users and end users to effectively and productively continue the use of SIROMS. CGI, as a result of having been directly involved with the development of the modules that comprise SIROMS, is well positioned and qualified to produce training materials, perform training sessions, maintain an environment for training, and administer efforts related to training.

As requested by DCA-DRM, CGI may deliver training sessions tailored to the needs of the attendees. Each session may include a combination of instructor presentations, hands on sessions within the module, PowerPoint slide decks, checklists, group Q&A discussions, session surveys for evaluation and feedback and email follow up. Recorded trainings may also be used. The CGI team will maintain a testing environment with production like code and data which will allow training to be administered and allow students to practice what they are taught. Requests for training and/or new or updated materials should be submitted five (5) business days prior to the expected training delivery date.

On an annual basis, CGI will coordinate with DCA to provide a session on industry-related solutions in the marketplace. CGI will work with DCA to determine any specific information or solution they may want to understand in more detail but, if not, will propose topics for discussion, with an emphasis on Commercial off the Shelf (COTS) software solutions. We envision leveraging our Emerging Technology Team, a group of seasoned IT professionals focused on the most cutting-edge technologies, to assess emerging technology tools and trends which can aid the State in ongoing disaster recovery efforts.

2.2.7 IT Practices, Data Security, and Integrity

CGI's enterprise security management services encompass the governance, strategies, frameworks, plans and assessments necessary to create and manage an effective enterprise-wide security program. Our focus is to work with our customers to articulate the appropriate governance and policies to achieve enterprise goals. With our systematic approach, CGI establishes an overall risk management framework that takes into account the unique risk profile of SIROMS and the associated regulatory and privacy requirements.

Security management goes beyond the physical levels that provide the access and control mechanisms for the facilities or infrastructure. It applies to protection of the software, applications, and data from corruption, or unauthorized intrusions, in order to maintain integrity. Dealing with these possibilities involves the analysis of potential threats and requirements surrounding the level of protection needed by the State to help ensure data confidentiality and integrity as well as service availability.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

The CGI team will continue to work closely with the State of New Jersey to properly secure the PII stored in SIROMS including the requirements specified in N.J.S.A 56:8-161 through N.J.S.A 56:8-166. In addition to these requirements, all systems are categorized based on which do or do not contain PII. All databases containing PII use transparent data encryption to help ensure that data at rest is encrypted.

DISASTER RECOVERY

Disaster Recovery is described in detail in section 2.2 of the Disaster Recovery and Contingency Plan (Appendix C).

BACKUPS

Database and Infrastructure backups are described in detail in section 2.1of the attached Disaster Recovery and Contingency Plan (Appendix C) and section 6.8 of the attached Infrastructure Overview document (Appendix E).

ENCRYPTION

Encryption of transmitted data is described in section 3.5.3 of the attached Security Plan (Appendix D).

DATA CENTER INFRASTRUCTURE

The SIROMS infrastructure will be maintained in three AWS Virtual Private Clouds, with UAT and Production in one region, AWS GovCloud (US-East), and DR in the AWS GovCloud (US-West) region. This environment is routinely referred to as platform as a service (PaaS). The operating system on all servers is either Windows 2019 or Windows 2022. These logical servers are AWS EC2 instances. There will be 8 servers in the UAT environment, 12 servers in the production environment and 1 server in the disaster recovery environment.

All AWS data centers feature:

- **Redundant systems** - N+1 redundant cooling, power, and telecommunications.
- **Backup power -** Uninterruptible Power Systems (UPS) prevent power spikes, brownouts and surges. Multiple diesel generators provide power in the event of a utility power outage.
- **Automated monitoring -** Extensive monitoring process of network, servers and applications to detect problems, often before they affect availability and to support capacity-planning services to accurately distribute and accommodate load.

- **Fire suppression system -** Zoned dry pipe fire suppression system (pre-action), a zoned under floor fire suppression system, smoke and fire detection systems, independent heating, ventilation and air conditioning (HVAC). All systems operate independently
- All AWS hosting facilities severely limit access to any visitors, including AWS venders and have state of the art monitoring.
- AWS also maintains and continuously monitors redundant HVAC systems

DATABASE

The SIROMS Database is designed as an OLTP Highly Scalable Transactional Database processing thousands of user queries a day efficiently, catering to the business user community of over 550 active users. The SIROMS Database servers will be hosted within AWS Cloud.

AWS Cloud

The AWS Cloud ® is a fully secure, fully managed cloud infrastructure environment that AWS' US East 2 and US West Government regions. The underlying infrastructure is FedRAMP moderate certified environment.

Database and Version

With the initial implementation of SIROMS in 2013, Microsoft SQL Server 2008 R2 was chosen as the database which best suited for the proposed solution. In keeping with best practices, the CGI team is constantly reviewing and planning Microsoft SQL upgrades to institute new features and functionality compatible with the rest of the SIROMS SaaS infrastructure.

SIROMS Database Servers

The SIROMS Database Server Architecture is on two different domains. The Development Environment is hosted on a CGI internal domain and the UAT, Staging, Production, and DR Environments are hosted on the FedCloud Domain. As the Development Environment is not located within a FedRAMP moderate level hosting facility, production data cannot be copied to it. We use three dedicated Database servers – Production Database server, UAT Database server, and DR Database server. UAT Database Server have corresponding UAT and Staging environments. The UAT and QA/Staging database environments are refreshed with Production data at least once a month, and on-demand as necessary to support development activities.

The SIROMS Database Server Architecture will be migrated to host on the AWS public cloud infrastructure utilizing CGI Federal's Active directory domain controls.

Disaster Recovery Server

As a Disaster Recovery Solution, all of the SIROMS Databases are mirrored on the DR Server using Always On Availability Group Configuration. For the safety of sensitive data, Always On Availability Group is configured with Live Transactional High Safety Synchronous Mode, which commits each of the transactions to DR Server (Secondary Server) before committing on actual Production Server (Primary Server). For Always On Availability Group status monitoring, automated SQL alerts have been configured.

SIROMS Database Security Policy

The Transparent Data Encryption (TDE) is enabled for the SIROMS Application Database in order to comply with the State of New Jersey's Security Policies and Requirements. The TDE is at the Database File level, so Application Database Data, Log, and Backup Files are encrypted using TDE, which require Encryption Certificates/Keys in order to Migrate/Restore Database on another Database Server. SIROMS Application Database cannot be restored/attached to another Server without an Encryption Key/Certificate.

Database Maintenance

All of the Databases are configured for an Integrity Check every morning before business hours, which provides information about any errors and overall health of the database. All of the Indexes/Statistics on all of the database tables are configured to Rebuild/Reorganize/Update weekly in order to consider weekly changes on data for Performance improvement. Additionally, the Database Admin and Support team tune the databases periodically and tune resource intensive SQL Queries as necessary.

Database/Server Monitoring

Automated SQL Alerts are configured for Database Server Performance, Deadlock/Blocking Events, etc. The SQL Alert Logs and Error Logs are configured to save SQL Queries on particular events for later analysis and troubleshooting purposes.

The Database Team actively monitors CPU/Memory Usage and Database Fragmentation for performance on daily basis, and performs Databases File Shrink, releases unused space to OS in order to maintain Drive Space on Database Servers, etc. In addition, all SIROMS Database Servers are actively being monitored for System/User Errors and Performance Threshold as part of the IPcenter Tool, one of the many CGI IP.

DATA INTEGRITY

Data Integrity refers to the completeness, consistency, and accuracy of data while created, transmitted, and stored. This means that the data should be intact and unchanged between updates of a data record. Data integrity can be maintained by the use of various validation procedures and error checking. The data integrity on the SIROMS project is verified through checksum algorithms which are derived from the digital data for the purpose of detecting errors which may have been introduced during transmission or storage. Before and after business hours, checksum reports are sent to the database team for verification.

LOGGING/AUDITNG CONTROLS

CGI understands the importance of logging and auditing to keep track of changes to the system, CGI has implemented logging and auditing at various levels to help ensure that we have the capability to answer any audit related questions.

Key application data tables with non-static data are tracked using SQL Server's Change Data Capture (CDC) module. CDC captures insert, update, and delete activity that is applied to a SQL Server database table. Both column information and metadata is stored in CDC tables which can be consumed for further analysis and auditing purposes.

All of the SIROMS database changes captured with CDC are stored in dedicated audit log tables. The audit log tables provide an audit trail of security-relevant chronological records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Since the implementation of CDC in 2015, a total of more than 610,000 jobs have been executed to move the appropriate data to the audit log tables. These jobs have processed almost 15 million CDC rows capturing over 24 million data points for audit tracking.

To help ensure continuous processing throughout the day, and to avoid backlog of these jobs, several status reports are configured to be sent to the database team during the day to provide alerts on any potential issues.

The CDC stored procedures create dynamic SQL to move the data changes to the various audit logs for each table that is tracked by CDC. This enables the addition of newly created tables to the process in less than 10 minutes when new functionality is developed by defining the metadata attributes in the CDC architecture, maintaining the high scalability and re-usability of the CDC process.

When Data Definition Language (DDL) changes occur to tables that are already tracked by CDC, a simple stop and start of the CDC tracking on that specific table will add the attributes that were added or removed.

The Transaction log generated are preserved and versioned using the backup processes described in the backup policy section below.

BACKUP POLICY

All of the SIROMS databases are configured for a full daily backup and a transactional hourly backup. A database can be restored up to the last full hour by restoring the full daily backup and the incremental hourly backup files. Apart from the backup configuration, the SIROMS databases are configured for Real Time Transactional Database Mirroring on the DR server, which commits and saves data on the DR server databases before committing on the Production server databases which assures that the SIROMS databases have an almost no data loss in case of an emergency or disaster.

2.2.8 Functional Requirements

For over 11 years, CGI has partnered closely with DCA-DRM on the SIROMS project, building a team of functional and technical experts who deeply understand the business processes and reporting needs essential for implementing DCA-DRM's disaster recovery programs. Our functional team brings a wealth of knowledge gained from supporting multiple grants and implementing dozens of programs, equipped with insights and lessons learned over the years. Having evolved along with DCA-DRM in disaster grant management expertise, CGI understands DCA-DRM's priorities and the nuances of how the organization approaches SIROMS development. This long-standing partnership means that CGI will seamlessly continue ongoing maintenance, updates, and supports efficient delivery of operations and services from the first day of contract award, without any interruption in service. To accomplish this, the CGI Team provides a diverse set of services described below.

APPLICATION SOFTWARE MAINTENANCE

The maintenance required for existing features and functionality will include, but is not limited to:

- Maintaining and updating documentation on changes to current functionality

- Modifying applications deployed in production to correct faults, to improve performance or other attributes
- Modifying the system to cope with changes in the software environment
- Increasing software maintainability or reliability to prevent problems in the future
- Maintaining and updating database objects
- Maintaining and updating software using Metastorm BPM v9.5, including scripting and workflow design, with implementation and maintenance of workflow systems for SIROMS BPM Applications
- Maintaining and updating client-side scripting using Javascript/JQuery/.NET for front end forms development
- Modifying SQL stored procedures and writing needed queries in MS SQL Server for updating SIROMS BPM and .NET modules and integration between them where required
- Managing, planning, and scheduling software builds for various applications through Test, Staging, and Production environments
- Tracking and controlling changes in applications, using Tortoise SVN Version Control System
- Maintaining and upgrading server, software, services, and database patching
- Managing OpenText Designer Studio builds for the purpose of deployment

PRODUCTION SUPPORT

The list of custom modules that comprise the SIROMS suite of software applications require varying levels of production support in order to diagnose, triage, troubleshoot, and resolve issues reported by end users. For instance, various recurring tasks are performed to verify that data from external, asynchronous systems is accurately and efficiently imported into the SIROMS on a day-to-day basis. SIROMS Production Support is essential to the support of over 50+ modules that comprise the SIROMS recovery system and maintain SIROMS as the system of record.

The inventory list of ongoing maintenance tasks related to Production Support will include, but are not limited to:

- Tier 1 to Tier 3 support as defined in Helpdesk section.
- Examples of reoccurring tasks will include, but are not limited to:
  - Addition of new fields and reason codes required to support program needs
  - Addition of new validations to help ensure data integrity
  - Handling requests for moving grant applications to and from various points in their respective workflows via database updates and script execution
  - Data migrations from external data sources
  - Imports of financial transactions which do not originate in SIROMS
  - A1 File Generation and NJCFS Integration for automated transfer of grant payments to the treasury system
  - Modifications to funding classifications via database updates in support of DRGR Reconciliation
  - Mass upload and/or reclassification of attachments/supporting documentation to grant applications

The following modules will be supported by one or many of the tasks detailed above:

- BPM Modules
  - Grant Management and Related Modules

  - Atlantic City Resiliency Program
  - Baseline Site Inspection
  - Blue Acres
  - Contractor Incident Tracking
  - Easement Acquisition Management
  - Environmental Review
  - ESGA - Phase I/Phase II/Phase III Applications
  - Flood Hazard Easements
  - Flood Hazard Risk Reduction and Resiliency
  - Forbearance
  - Grant Program Management
  - Ida Housing
  - Ida Map
  - LMI
  - Local Planning Services (LPS)
  - LPS Zoning
  - LRRP
  - Mitigation Assistance
  - National Disaster Resiliency Program
  - Resilient Communities
  - RREM
  - Site Inspections
  - Smart Move
  - Strategic Recovery Planning Report
  - Supplemental Fund
  - TBRA
  - Uniform Relocation Act (URA)
  - USD

- Finance Management
  - A1
  - Accounts Receivable
  - Contractor Invoice Module
  - Forecasting
  - Forecasting Data Integrity Tool
  - Funds Request
  - IFS Activation Management

    - IFS QPR Management
    - IFS Status Management
    - Multi-Applicant Invoice (MAI) Module
    - Payee/Vendor Management
    - Payment Request
    - Program Income
    - Return Funds

  - Reporting
    - Federal Reports (FFATA, Section 3 and WMBE)
    - Measure Reporting Management
    - Quarterly Performance Report – Measure Reporting
    - Technical Assistance and Monitoring
    - VCA-LEP Quarterly Reporting

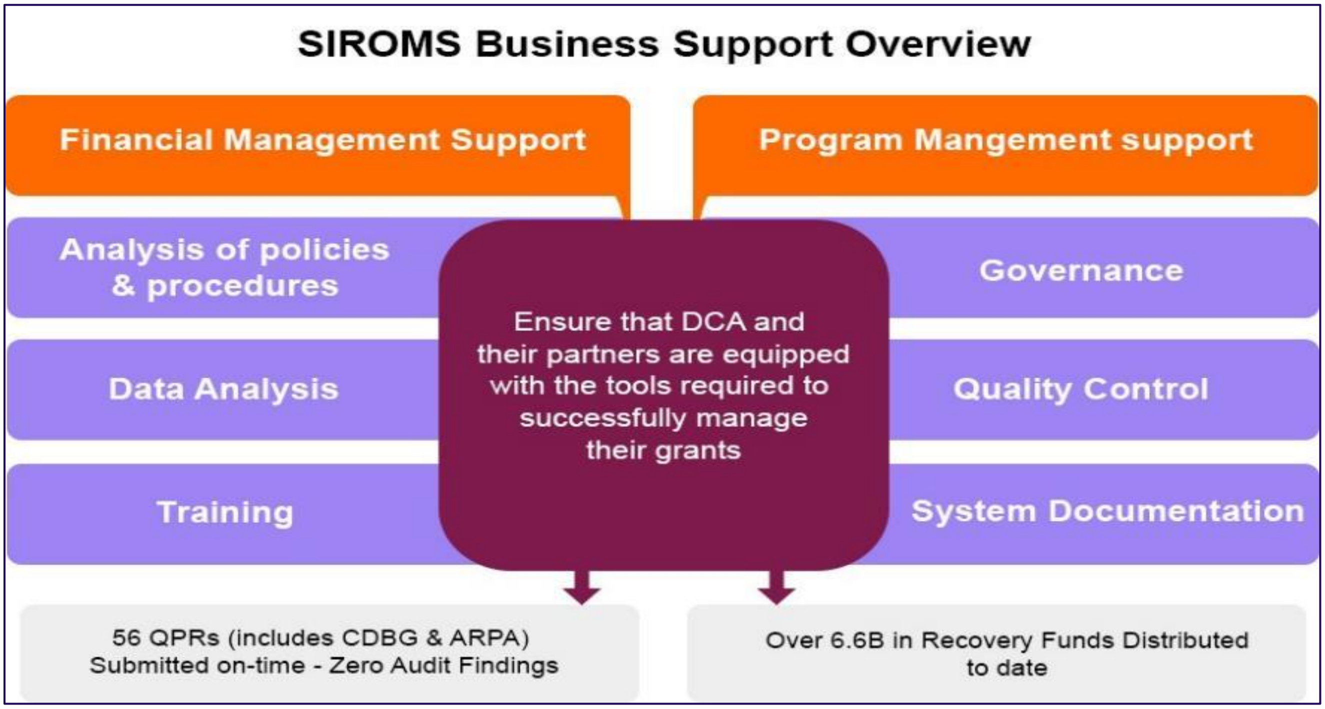
  - American Recovery Plan Act
    - ARP Master Program (AMP)
    - ARP QPR
    - Grant Management Reporting
    - Project Expense Reporting
  - Change Request
  - Reference Library
  - User Access Request

- .Net Applications
  - ACH Escrow Overpayment Return
  - ACH Transaction Processing
  - Flood Hazard Risk Reduction Public Application Intake
  - Housing Counseling Services
  - Lead Hazard Reduction Program Environmental Review Request Tool
  - LMI Public Application Intake
  - Public Portal
  - Rental Assistance Program Application
  - Resettlement Archive
  - RREM Waitlist
  - Section 3 Vendor Portal
  - SIROMS Appointment
  - Sweeney Applicant Status Form

BUSINESS SUPPORT

As the primary grantee of multiple recovery and mitigation grants, DCA-DRM, in coordination with its partners, is responsible for the oversight and execution of multiple programs within multiple grants across the state. Much of the day-to-day operations for these programs is documented, organized, and managed within the SIROMS suite of applications. Meeting the technology needs of a diverse user base of this size requires significant Business Support.

Exhibit 14 - SIROMS Business Support Overview


SIROMS Business Support Overview
Financial Management Support
Program Mangement support
Analysis of policies & procedures
Data Analysis
Training
Governance
Quality Control
System Documentation
Ensure that DCA and their partners are equipped with the tools required to successfully manage their grants
56 QPRs (includes CDBG & ARPA) Submitted on-time - Zero Audit Findings
Over 6.6B in Recovery Funds Distributed to date

CGI's Business Support model will help ensure that the software continues to provide the flexibility required by the state's ever changing business needs and to handle exception cases. The tasks that the CGI team may undertake in order to provide Business Support to DCA-DRM and its partners include, but are not limited to:

- Prepare for and conduct or participate in PMOs/status meetings
- Client stakeholder communication management at all organizational levels
- Issue analysis, troubleshooting, escalation and remediation
- Delivery of ad-hoc training, one-on-one or to small groups
- Analysis of new, or proposed new/modified, policies and procedures to determine system impacts or potential system impacts
- Document types/scanning convention maintenance and configuration
- Map work function(s) to existing user roles, update for new employees or role changes, and other user access management updates.
- Develop and confirm of ad-hoc reporting requirements and delivery of reports
- Develop and distribute of data migration templates, and associated collection, validation, and processing.

REQUIREMENTS MANAGEMENT

The state may require system and/or reporting development and/or enhancements that originate from various sources, including but not limited to:

- Action Plan and Action Plan Amendments
- State legislative actions
- Unanticipated requirements from the State of New Jersey, US Department of Housing and Urban Development, US Treasury or other federal entity
- Changes deemed necessary by users as a result of more sophisticated use and knowledge or evolution of program.

Requirements may be defined for any number of modifications that include new or modified code, including adding or updating:

- Modules to support new programs
- Data and management reports to support the administration of programs, management of finances, and federal reporting requirements
- Interfaces to other critical systems
- Websites to provide and/or collect program data

Due to the dynamic nature of disaster recovery and DCA-DRM's need to meet the requirements of various external stakeholders, the CGI team recognizes the need for a time boxed, iterative approach to software delivery in line with a hybrid Agile methodology. A hybrid Agile methodology will allow for rapid software development; with software changes typically taking place within a four-week iterative cycle.

The process begins with the identification of a need and the submission of a Change Request (CR) in SIROMS. A CGI business analyst will analyze the change and facilitate Joint Application Design (JAD) sessions with appropriate DCA-DRM staff to elicit change prerequisites and conditions. Subject matter experts identified by DCA-DRM are expected to attend these JAD sessions and provide the input necessary for CGI business analyst to understand the business need and desired outcome. CR requirements are derived from the JAD sessions to form the basis of a Business/Functional Requirements Document (BFRD). Depending upon the nature of the change, the BFRD will address the following components:

- Business Objective
- Business Process Analysis
- Detailed Requirements
- Screen Mock-Ups
- Design Specifications
- Proposed Process Flows
- User Role Definition
- Field Level Mapping
- System / User Testing Considerations
- Reporting Specifications
- Reference Documents

During BFRD development, the business analyst will socialize the change with the CGI cross-functional teams including development, reporting, database, interface, and quality control. Feedback from the subject matter experts on these teams will be incorporated into the requirements, where applicable.

Once a draft BFRD is complete, it will be reviewed with DCA-DRM and updated as needed until the content is finalized. Once completed, DCA-DRM will be required to approve the BFRD before development work begins. Finalized BFRDs will be posted to the appropriate SIROMS Change Request folder for final approval to proceed with development.

The detailed requirements in the approved BFRD will be used by the development and QC teams as the basis for system development and QC script development. Any necessary clarifications or modifications to requirements will be provided to the development and QC teams by the Business Analyst and may require additional DCA-DRM feedback.   Any subsequent changes to the BFRD after DCA-DRM approval will be documented and a revised version of the BFRD will be posted to the SIROMS Change Request folder.

2.3 Tasks and Deliverables

2.3.1 Role of Contractor- Startup

As the incumbent vendor, CGI is uniquely positioned to seamlessly transition into the new contract. As indicated in the mobilization plan, the project will continue to be staffed by our experienced CGI Partners, who have been integral to the SIROMS project for years. This group of primarily local professionals possess deep institutional knowledge and extensive experience in enhancing and maintaining SIROMS. Given their familiarity with the project and their roles, no transitional training or knowledge transfer will be necessary. The CGI team is prepared to assume all SIROMS-related tasks and hosting responsibilities from day one. Although we do not foresee the need for training or knowledge transfer, CGI will prepare a schedule of activities within the first 10 days that will be reviewed as part of the project kick-off meeting identified in the mobilization plan. The intent is to help ensure that CGI and DCA-DRM are aligned on upcoming tasks associated with the initiation of the new contract.

2.3.2 Contractor Staffing

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

2.3.3 Contract Closeout

Upon conclusion of the Contract, the CGI PM will work with the SCM to organize and conduct a closeout meeting or series of meetings. During this/these meeting(s), the CGI PM will provide a Status Report, in a format to be mutually agreed upon by SCM and CGI PM, that details the completeness of each deliverable successfully completed during the period of performance of the associated contract. Upon approval of this report, the CGI PM and SCM will mutually agree to a schedule in which all project documentation will be handed over to the State and the format in which it will be turned over.

During this period of time, CGI will also provide transitional support and training to the State as requested. Per the requirements of the RFQ, CGI also agrees to transfer any licenses and provide administrative access to each core software component to the State upon conclusion of the contract.

2.4 Technical Environment

2.4.1 State Technology Requirements and Standards

SIROMS will be hosted within the AWS GovCloud environment whose underlying infrastructure is fully FedRAMP certified. This system complies with the guidance of the *NJ Statewide Information Security Manual: https: //www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf* . The environment will be audited yearly for NIST 800-53 compliance as required by the State.

If requested by the State, CGI will be an active participant and provide any existing architecture documentation to DCA-DRM in support of NJOIT’s System Architecture Review process. In addition, CGI will support the State in any audits conducted for SIROMS.

The SIROMS suite of applications was initially developed over 10 years ago and will be hosted by the vendor in its own AWS VPC. As such, fully meeting the web presence guidelines will require significant effort to complete. We recognize the value in presenting unified branding across the state’s various web sites. Existing public facing applications in SIROMS have been developed to match the state guidelines as much as possible. CGI will work with DCA-DRM to identify and prioritize any further updates to the system to allow it to meet these standards.

As part of all future changes, CGI will use IBM Accessibility Checker to verify that all changes made to the application conform to WCAG 2.0 Level AA. This browser-based plug in provided by IBM that performs checks against several accessibility standards, including WCAG 2.0. DCA-DRM will be informed of any issues that are identified so that fixes to them can be prioritized as part of the SDLC.

SIROMS uses LDAP authentication that is provided by LDAP servers hosted as part of the SIROMS environment for internal users. For external applicants, usernames and passwords are established as part of the process for registering with the programs that they are participating in, and emails are used to provide a second authentication factor. CGI will work with the state to determine the feasibility of moving its user authentication strategies to the state recommended methods and will inform DCA-DRM about any impact this change will have on the various user groups in the system.

2.4.2 System Design

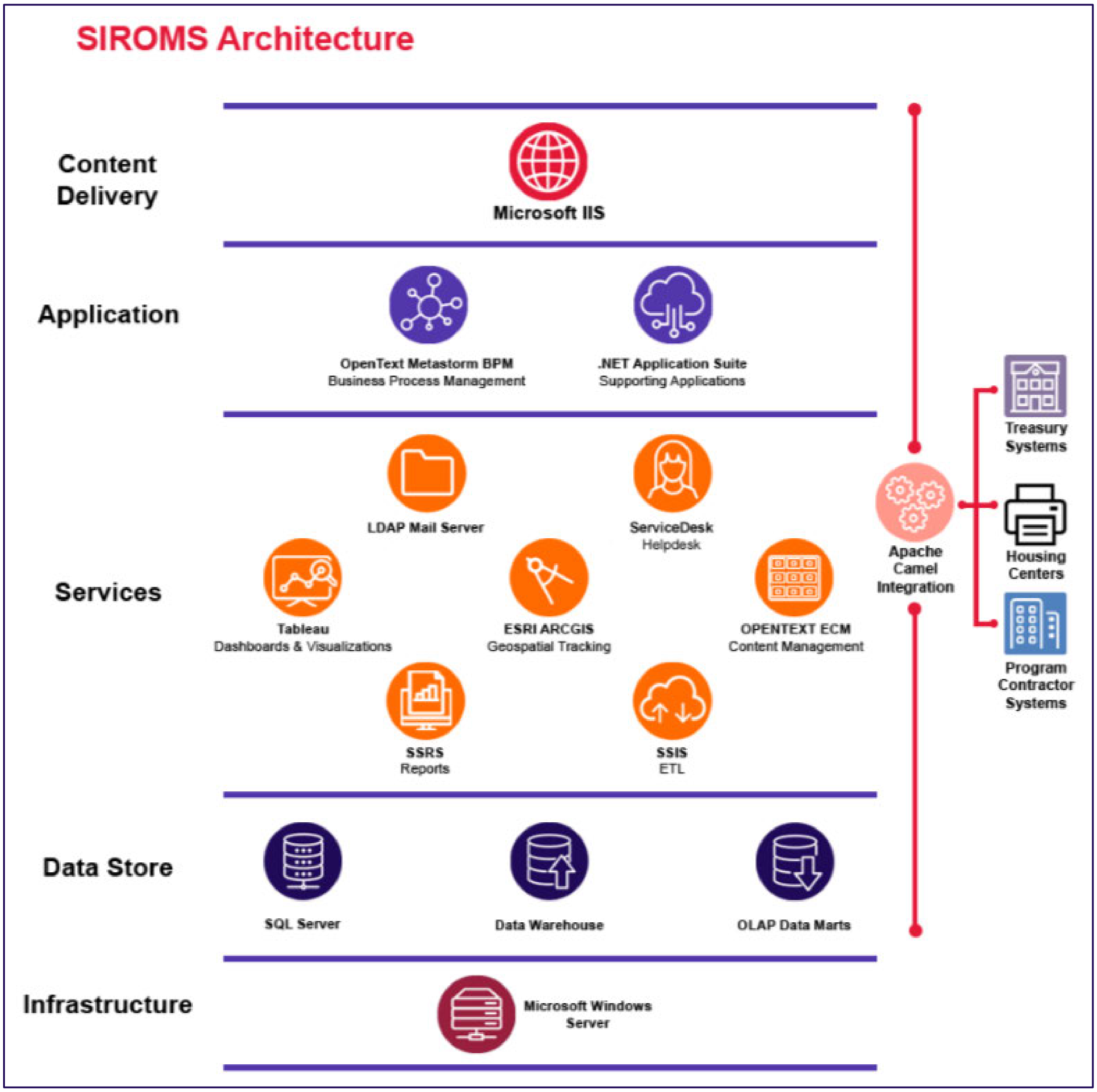
SIROMS is a proven system for managing thousands of emergency funding applications and disbursements, while enabling federal compliance. CGI understands well how the SIROMS system is adaptable to unique program requirements and will be able to leverage our expertise and institutional knowledge to take advantage of the following features:

- A web-based portal to simplify management of funding requests while enabling citizens to complete applications for assistance and track status online
- A collaboration portal allowing other state contractors and departments receiving CDBG-DR grants and other disaster recovery funding to provide reports necessary to accomplish and fund their projects
- Business process management software integrated with data warehouse and business intelligence systems for in-depth analysis of funding distribution and outcomes
- Financial management integrated with the State Treasury system
- A full lifecycle grant management system allowing the State to track an application from intake through closeout
- AWS's secure government cloud infrastructure, which reduces setup time and complexity, and provides the 24/7 reliability needed for a large-scale disaster recovery program.
- Highly automated workflows to minimize application processing time, enforce compliance, and report program results to federal agencies
- Comprehensive, ad-hoc and pre-built reporting to support State recovery programs
- Single virtual file for tracking and managing all data for an application, ensuring consistent records for auditing and reporting purposes

The SIROMS system is built using proven technologies, such as OpenText Business Process Management (BPM), and Microsoft .NET, chosen by CGI to meet the fast moving and scalable needs of a Disaster Recovery program. The core of the back-office functionality is built on BPM. **BPM provides workflow-driven management of the business processes of any DR program or administrative function, providing clear visibility into the progress, current status, and task ownership for any given record.** BPM also facilitates rapid system design and development; this allows us to reuse specific modules from the existing SIROMS software base to create new modules when necessary. CGI has also utilized the .NET Framework on components of SIROMS, which require less complex workflow and greater flexibility from a User Interface (UI) perspective.

CGI will continue to implement the following SIROMS Architecture that has facilitated the successful management of the New Jersey State Recovery programs.

Exhibit 15 - SIROMS Architecture



2.4.3 Hosting and Backup Services

CGI hosts SIROMS within the AWS GovCloud cloud infrastructure, whose underlying structure is FedRAMP Moderate certified, and CGI will maintain and verify NIST 800-53 rev. 5 or higher compliance of the SIROMS SaaS solution.

CGI will provide comprehensive backup services in the form of database backups via MS SQL Server and full and incremental system backups using MS SQL server scripting and a state-of-the-art AWS backup tool for all EC2 instances that maintain the SIROMS SaaS. Data can be provided to the State at any time in the form of MS SQL Server database backup files and database log files as well as documents. The full details of these backup services, including monthly system backups of all production virtual machines, can be found in the attached –*Appendix E Infrastructure Overview* and Appendix C Disaster Recovery and Contingency Plan

2.4.4 Extranet Plan

The proposed SIROMS SaaS, which will be hosted in the AWS GovCloud and will utilize multiple IPsec tunnels from the Palo Alto firewalls that control ingress and egress from the SIROMS SaaS to OIT facilities to emulate MPLS connections. This will require OIT to work with the CGI networking team to form IPsec tunnels with OIT firewalls. These IPsec tunnels will be able to securely provide the bandwidth required to transfer most data that might be currently transferred via MPLS lines. If DCA-DRM determines that they need to increase the amount of data being transferred from the SIROMS SaaS hosted in the AWS GovCloud to NJCFS or other New Jersey state departments, which might require higher performance data transfers, CGI can negotiate the equivalent of MPLS dedicated links (public cloud providers do not allow direct MPLS connections to their infrastructure) to the AWS VPCs that will host the SIROMS SaaS at additional costs. These MPLS equivalents are known as AWS Direct Connect. The costs for AWS Direct Connect would be based on creating the Direct Connect connection, which is directly related to performance parameters of the Direct Connect, plus the amount of data transferred over the connection(s).

2.4.5 Transmission of Files

SIROMS data will be hosted on Windows 2019 and Windows 2022 servers, which require SFTP for secure transmission of data. A Cerberus SFTP server has been set up and tested in both the production and UAT environments allowing secure synchronous data transfer between the CGI and the state on ports 21 and 22 via FTP, SFTP and FTPS. This allows CGI to send and receive data on demand. If the state should ever require a repetitive transfer of data, this could be scheduled to meet the state’s requirements. SIROMS does not currently have a requirement to provide asynchronous file access. CGI will work with the SCM to implement a file transfer approach with the State of New Jersey IBM mainframe that meets their security requirements.

In addition, SIROMS system files, in the form of AWS EC2 clones are created on a regular basis and transmitted to the disaster recovery region, GovCloud (US-West), into an encrypted backup vault.

2.4.6 Automated Records Management/Storage Systems and Related Services

Any requests for SIROMS information falling under the Open Public Records Act (OPRA) is recorded as a Helpdesk ticket so the work required to service the request can be properly tracked and audited. An email will be sent to the SCM for any OPRA request to be fulfilled by the State OPRA Custodian.

SIROMS utilizes OpenText Content Server (ECM) for storing and managing over 2.3 million documents, certified by NJ's Division of Revenue and Enterprise Services, and will comply with the State's record retention schedule for Record Series Number 0406-0001. CGI will work with the State to maintain DORES certifications.

2.5 Assessments/Plans

2.5.1 Disaster Recovery Plan

CGI will provide final updates to its existing Disaster Recovery and Contingency Plan and deliver it to SCM for review well in advance of the 30 business days after Contract award. An initial draft version of the updated Disaster Recovery and Contingency Plan is included as Appendix C.

2.5.2 Contingency Plan

CGI will provide final updates to its existing Disaster Recovery and Contingency Plan and deliver it to SCM for review well in advance of the 30 business days after Contract award. An initial draft version of the Disaster Recovery and Contingency Plan is included as Appendix C.

2.5.3 Performance Management Plan

CGI will provide final updates to its existing SIROMS Performance Management Plan and deliver it to SCM for review within 30 business days after Contract award. An initial draft version of the updated Performance Management Plan is included as Appendix B. The Performance Management Plan will be updated annually to reflect any changes mutually agreed upon between CGI and DCA-DRM and it will follow established review and approval processes before being made final.

The Performance Management Plan proposes the jMeter tool for automated stress testing and includes recommended benchmarking methods, benchmarking metrics, and measurable goals. The plan also proposes a variety of resolution methods depending on issues that may arise. Finally, the plan does describe how CGI can meet the specific service metrics and expected service levels set forth in section 4.5.3 of the Request for Quote. CGI will provide performance testing results within 20 business days of a request by the State.

2.5.4 Potential Cost Savings

Through our experience working closely with the State and DCA-DRM in support of their mission to assist New Jerseyans and their communities recover from the devastating impacts of Superstorm Sandy, COVID-19, and Hurricane IDA we fully understand that it is the duty of the State to simultaneously utilize the recovery funding as efficiently as possible in an effort to maximize the impact of the recovery programs it administers while also acting as a steward of the American tax dollars which are funding the recovery efforts. Our experience as the only Vendor experienced in the design, development, implementation, maintenance, and support of the SIROMS system also provides us with unique insight into the system and its various applications. Should we be fortunate enough to be selected to continue to serve the State and DCA-DRM in the management of the SIROMS solution, CGI proposes to conduct a meeting with the SCM and/or his designees, within the first 30 business days after contract award, to discuss the requirements and terms we believe fulfill the State's business needs and may provide the State with potential cost saving opportunities should the State be willing to continue the negotiation of the requirements and terms.

3 Organizational Experience

3.1 Location

3.1.1 CGI's Client Proximity Model

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

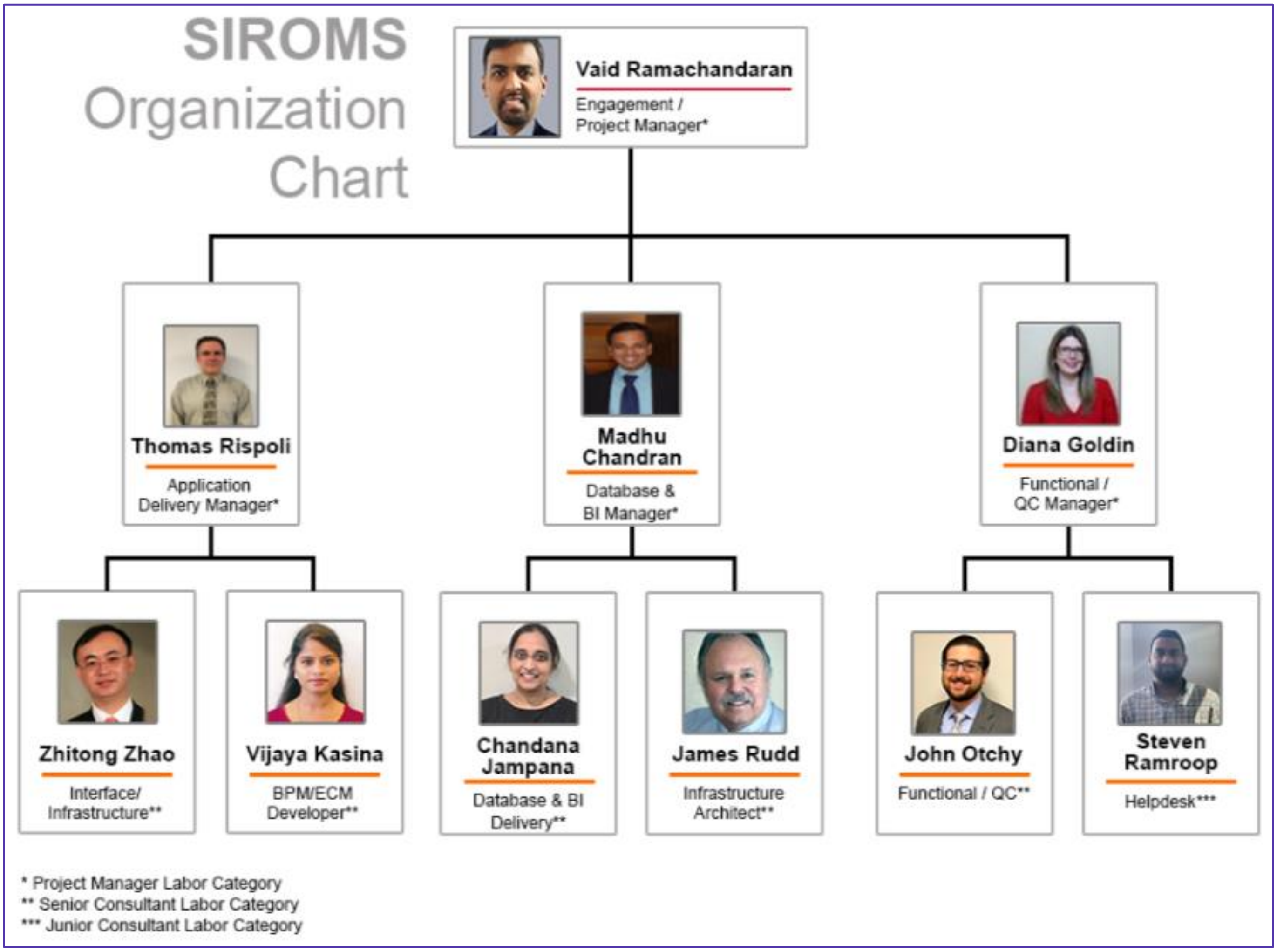
[redacted]

3.2 Organization Charts

The key personnel assigned by CGI for the maintenance of SIROMS have in-depth knowledge of the system. They have been directly involved implementing complex programs for SIROMS for years; helping to ensure it remains compliant with federal reporting requirements in an ever-changing environment.

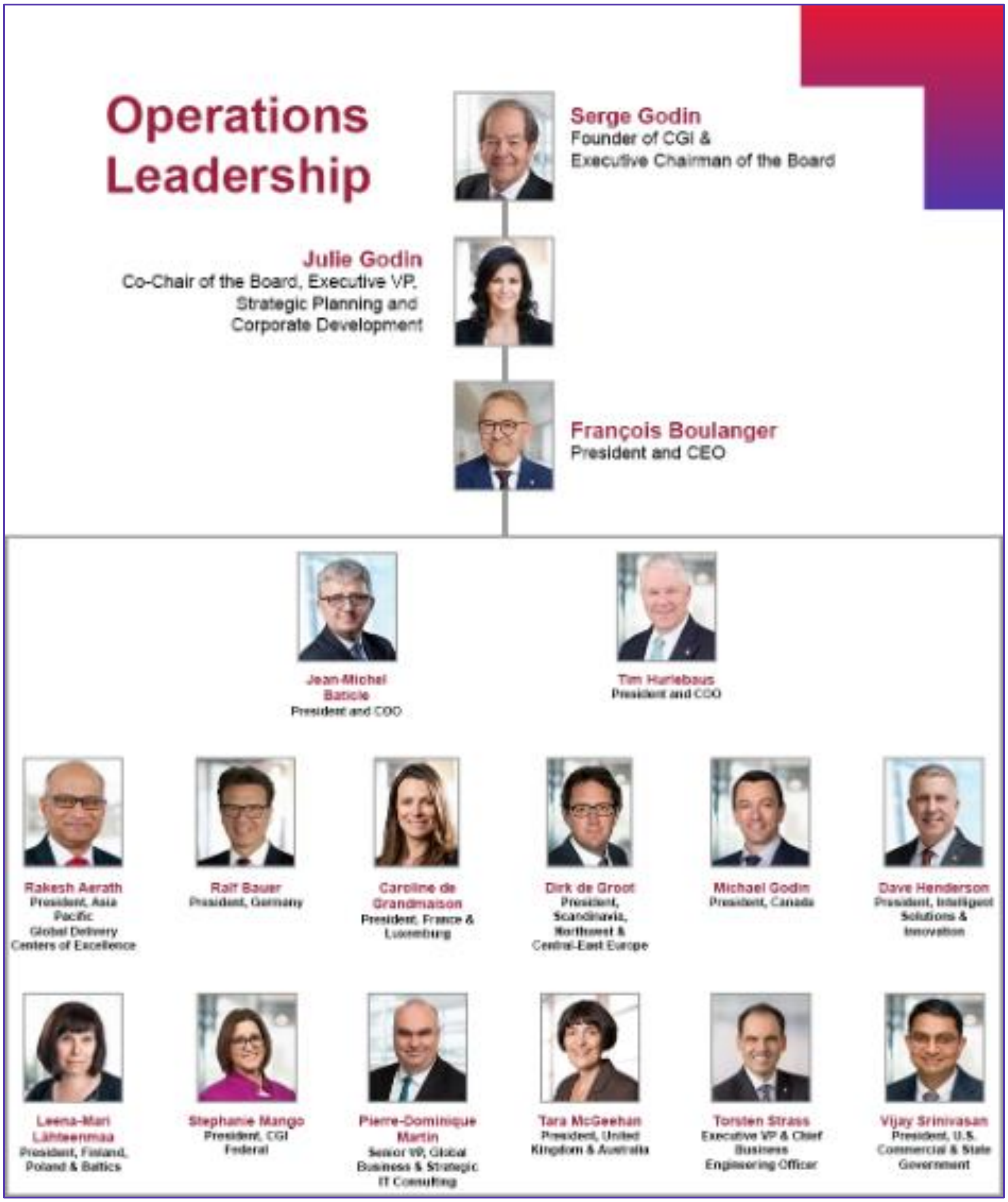
The key staff comprising the SIROMS project team is shown in Exhibit 16.

Exhibit 16 - SIROMS Project Team Key Staff



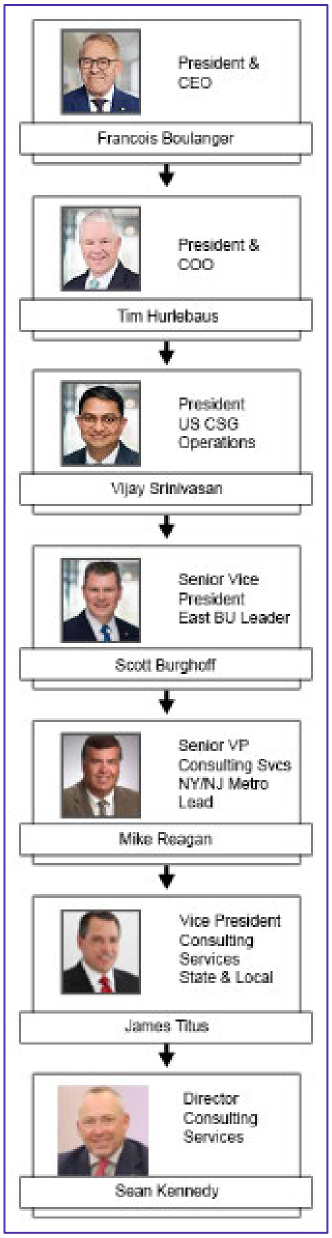
CGI’s Corporate Leadership Team is shown in Exhibit 17.

Exhibit 17 - CGI Leadership Team


Operations Leadership
Serge Godin
Founder of CGI & Executive Chairman of the Board
Julie Godin
Co-Chair of the Board, Executive VP, Strategic Planning and Corporate Development
François Boulanger
President and CEO
Jean-Michel Baticle
President and COO
Tim Hurlebaus
President and COO
Rakesh Aerath
President, Asia Pacific Global Delivery Centers of Excellence
Ralf Bauer
President, Germany
Caroline de Grandmaison
President, France & Luxembourg
Dirk de Groot
President, Scandinavia, Northwest & Central-East Europe
Michael Godin
President, Canada
Dave Henderson
President, Intelligent Solutions & Innovation
Leena-Mari Lähteenmaa
President, Finland, Poland & Baltics
Stephanie Mango
President, CGI Federal
Pierre-Dominique Martin
Senior VP, Global Business & Strategic IT Consulting
Tara McGeehan
President, United Kingdom & Australia
Torsten Strass
Executive VP & Chief Business Engineering Officer
Vijay Srinivasan
President, U.S. Commercial & State Government

The US Commercial and State Government (USCSG) Strategic Business Unit (SBU), which is lead by Vijay Srinivasan, as part of CGI Technologies and Solutions Inc., will be responsible for the SIROMS project. The key element of our management structure is the Business Unit (BU) within the USCSG structure. BUs are designed to respond effectively and efficiently to clients' demands. Based on our client proximity guiding principle, a BU has a geographic focus. The US East Business Unit, which would be delivering the SIROMS project, is empowered to manage its resources and to make decisions based on our global strategy, governance rules, policies, and management frameworks. The relationship between the individual assigned to lead the SIROMS project with the overall organization structure is shown in Exhibit 18.

Exhibit 18 – US Leadership Team


President & CEO
Francois Boulanger
President & COO
Tim Hurlebaus
President US CSG Operations
Vijay Srinivasan
Senior Vice President East BU Leader
Scott Burghoff
Senior VP Consulting Svcs NY/NJ Metro Lead
Mike Reagan
Vice President Consulting Services State & Local
James Titus
Director Consulting Services
Sean Kennedy

3.3 Resumes

CGI has a well-known track record of successful projects around the globe, drawing on a group of 91,000-strong CGI partners worldwide, providing professionals with the technical skills and functional knowledge that is required for successful implementations. CGI recognizes that the continued success of this effort requires experienced professionals who are familiar with the DCA-DRM environment and its data, are seasoned in technology project management, and have expertise delivering at DCA-DRM, specifically for the SIROMS project.

As stated previously, CGI will draw upon proven resources to fulfill management, supervisory, and key personnel roles. These resources have demonstrated they have the knowledge and skills to meet the requirements of the role he/she is designated to perform. Resumes submitted will list job experiences that demonstrate qualifications and experience completing contracts of a similar size and scope. As current SIROMS team members, these resumes will exhibit each individual's ability to contribute to successfully deliver the services required by this RFQ. Each relevant job experience will include beginning and end dates.

Proposed primary staff resumes are included in Appendix A.

3.4 Experience With Contracts of Similar Size and Scope

CGI is proud to provide the references below to demonstrate our highly relevant project experience with contracts similar in size and scope. There have been no negative actions associated with CGI’s work on any of these projects nor negative findings from any governmental agencies. Since we do not intend to leverage a sub-contractor for the SIROMS project, no sub-contractor references are provided.

3.4.1 Central Office of Recovery, Reconstruction, and Resiliency (COR3) Government of Puerto Rico

ENGAGEMENT DESCRIPTION AND OBJECTIVES

Since 2018, CGI has partnered with Puerto Rico’s COR3 to develop their Disaster Recovery Solution (PR-DRS), centralizing funding records from agencies like FEMA and HUD. This system supports financial management, grant management, and transparency. CGI also created the COR3 transparency portal, providing public access to recovery fund data through charts and maps.

Building on their success with post-hurricane recovery in other states, CGI’s work in Puerto Rico leverages previous investments in disaster recovery software, benefiting both Puerto Rico and other states. This initiative manages over $69 billion in federal recovery funds, marking one of the largest disaster-recovery technology efforts in the U.S.

CGI RECOMMENDATIONS

The solution leverages the SIROMS system, built with Business Process Management (BPM) and Microsoft .NET, to meet the dynamic needs of disaster recovery. BPM manages business processes, providing visibility into progress and task ownership, and allows for rapid system design and module reuse. The .NET Framework is used for components requiring flexible user interfaces.

Using a hybrid Agile approach, CGI collaborates closely with program management for a phased implementation of disaster recovery technologies. These are hosted on-premises in Puerto Rico at Evertec’s secure, regulatory-compliant Data Center to support the CRRO’s DRDMS project.

RESULTS

CGI developed and maintained the following comprehensive management systems:

- **Financial Management**
    - **Program/Activity Allocation:** Managed budgets and performance measures for multiple funding sources, helping ensure strict financial control and audit trails.
    - **Funds Requests:** Facilitated grant disbursements by aligning with HUD and federal structures, integrating with external systems for quick approvals.
    - **Accounts Receivables/Cash Receipts:** Tracked ARs and CRs, helping ensure funds were available for redistribution.
    - **Program Income:** Managed income from CDBG-DR programs, helping ensure compliance with HUD regulations.
    - **Financial Forecasting:** Standardized financial forecasting for recovery programs, providing visibility into funding needs.
    - **Contractor Invoice Management:** Managed contracts, tasks, invoicing, and accounts payable.
- **Grant Management:**
    - **Housing Rebuilding Program (HRP):** Centralized application data, property damage estimates, construction progress, and grant disbursements, tailored for compliance with PROMESA/FOMB guidelines.
    - **External Facing Application Intake:** Developed a multilingual webpage for storm victims to apply for recovery programs, integrating with the grant management system.
    - **Appointments Tracking:** Recorded scheduling and completion of meetings between applicants and program staff.
    - **Application Status Tracking:** Provided applicants with secure access to view their application status and interact digitally for additional documentation needs.
- **Reporting (Federal Reporting and Compliance)**
    - **HUD Quarterly Progress Reporting (QPR)**: Assists grantees in completing QPRs by compiling funding data, recording progress narratives, and detailing performance measures. This data can be directly uploaded to HUD’s DRGR system.
    - **Other Federal Reporting Requirements**: Collects and reviews data for various federal reporting needs, including FFATA, Section 3, and MWBE.
    - **Technical Assistance & Monitoring (TAM)**: Records and reports TAM occurrences for grantees and sub-grantees.
    - **Data Warehouse (DW)**: Supports reporting, transparency, and compliance by consolidating data using MS Business Intelligence, MS SQL Server, and CGI’s Integration Engine.
    - **Business Intelligence Reporting**: Provides timely, accurate, and actionable reports using SQL Server Report Builder and Web Intelligence, with over 300 report and dashboard templates available for immediate use.
- **Support Services**
    - **Constituent Services Tracking**: Records public requests for information about HUD-funded recovery efforts, managed by Call Center staff.
    - **Integration Engine**: Built on Apache Camel, it integrates disparate systems and is adaptable for Puerto Rico’s needs.
    - **Geospatial (GIS) Integration**: Provides geospatial visualization of recovery efforts, leveraging CGI’s experience with GIS-driven transparency tools.

  - **Collaboration**: Uses Microsoft SharePoint for policy and procedure documentation, including a custom Policy Change Request tool for workflow-based policy management.
  - **Document Management and Retention**: Utilizes OpenText Content Server for storing and managing over 2.3 million documents.
  - **Help Desk**: Employs ManageEngine ServiceDesk Plus for ITIL-compliant incident and problem management, with bilingual support available.
  - **System Change Request Tool**: Facilitates the submission, evaluation, and tracking of system functionality requests, supporting over 1,200 changes to date.

- **Cloud Hosting, On-Premises in Puerto Rico**: CGI provided a fully managed software infrastructure platform based in the locally-maintained Evertec Data Center. Built for security from the ground up, the Evertec Data Center met Federal and Puerto Rican regulatory requirements for sensitive data collected through the management and execution of DR programs. It also provided the availability and scalability required to accommodate the needs of the DRDMS project. CGI proposed the Evertec Data Center in San Juan as the primary site for hosting the DRDMS solution and to leverage a Microsoft Azure US Data Center for the solution's Disaster Recovery environment, to provide geographic redundancy.
- **Alternate Primary Hosting Option – *Microsoft Azure*** – CGI was a Microsoft Gold Partner, as well as one of only a few Microsoft global system integrator partners in the world. If preferred by the CRRO, CGI could offer an alternate hosting option fully located in the Microsoft Azure Public Sector cloud.

Some of the key successes of CGI's partnership with the Puerto Rico's COR3 include:

- Obligated over **$36.8B worth of recovery and resiliency programs within Puerto Rico since 2018.**
- Disbursed over $10.1B through the FEMA Public Assistance program across over 20,000 individual payments
- Disbursed over $102.5M through the FEMA Hazard Mitigation Grant Program across over 1,000 individual payments
- Provides transparency into over $3.6B in funding made available through the American Rescue Plan Act and over $2.2B in funding made available via the CARES Act
- **1,049 FEMA Program Subrecipients** currently served through PR DRS
- Puerto Rico has successfully submitted **20 QPRs for Public Assistance** and **14 QPRs for Hazard Mitigation**
- CGI has assisted COR3 successfully pass multiple audits from multiple organizations including the Puerto Rico Office of the Comptroller and the federal Office of Inspector General and Government Accountability Office.
- 70+ executive dashboards and operational reports currently delivered on automated schedules

ENGAGEMENT REFERENCES

Central Office of Recovery, Reconstruction, and Resiliency (COR3) Government of Puerto Rico: Reference 1	
Name	Marlena Riccio Paniagua
Title	Deputy Director

Company	Central Office of Recovery, Reconstruction, and Resiliency (COR3), Government of Puerto Rico
Address	PO Box 195014, San Juan, PR 00918-5014
Phone Number	(787) 948-7010
Email Address	MRiccio@cor3.pr.gov

Central Office of Recovery, Reconstruction, and Resiliency (COR3) Government of Puerto Rico: Reference 2	
Name	Mayté Bayolo Alonso, Esq.
Title	PMO Director
Company	Central Office of Recovery, Reconstruction, and Resiliency (COR3), Government of Puerto Rico
Address	PO Box 195014, San Juan, PR 00918-5014
Phone Number	(787) 474-7050 ext. 1110
Email Address	MBayolo@cor3.pr.gov

3.4.2 State of New Jersey Department of Environmental Protection

CGI is pleased to have been a trusted partner to the New Jersey Department of Environmental Protection for nearly 30 years. During this time the NJDEP, together with CGI, has remained ahead of the curve by quickly adapting to changing technology to improve its service delivery, operational efficiency, and data reporting and analytics capabilities. In this way, the NJDEP has maximized the ways in which it can help to protect New Jersey's environment, promote the health of its residents and visitors, and lead the way nationally by providing modern communication channels to inform and engage with the public and regulated community. This section highlights the successes achieved by NJDEP as a direct result of CGI's consultation and support.

> "The CGI team continues to introduce innovative concepts, processes and tools that allow NJDEP to meet and exceed expectations relative to our ever-changing IT requirements and initiatives."
>
> **Pete Tenebruso**
> Chief Information Officer, NJDEP

ENGAGEMENT DESCRIPTION AND OBJECTIVES

Over the course of the past three decades, CGI and the NJDEP have worked closely together navigate a successful digital journey that has followed the path of some of the major milestones below:

- **1995** – CGI developed an idea for a technologically advanced enterprise-wide system that, which was introduced as the New Jersey Environmental Management System (NJEMS) in 1998.
- **2000** - The NJDEP Online business portal was launched to facilitate electronic submission of permit applications, reports, payments and more.
- **2002** – With the enactment of the Open Public Records Act (OPRA), NJDEP and CGI established an online public record request portal and internal Open Public Records Act Tracking

System (OPRATS) that has been instrumental in increasing engagement and transparency with the public.

- **2015 –** NJDEP Data Miner, an online reports portal supported by the NJEMS database, began to provide the public with a variety of reports with up-to-the-minute results from many environmental subjects.
- **2017 –** NJEMS Modernization Roadmap is developed to continue to evolve the NJDEP as an agency able to meet the challenges of the 21st century and deliver on its commitment to service excellence.

CGI RECOMMENDATIONS

Currently, the NJDEP and CGI are in the final phases of what has been a tremendously successful effort over the past six years to modernize its enterprise-wide back-office application, the New Jersey Environmental Management System (NJEMS), by leveraging the Pega business process management platform. This will bring modern technology, streamlined business processes, and Geographic Information System integration to the NJDEP as it continues to be a leader among state agencies in digital transformation.

Additionally, over the past couple of years CGI has been proud to support the NJDEP through its agile processes to quickly implement key initiatives within the state, including the first Environmental Justice program in the nation, as well as NJ PACT (Protecting Against Climate Threats). CGI consulted closely with NJDEP stakeholders to define new business processes to accommodate Environmental Justice provisions to minimize public health stressors within vulnerable communities and then incorporate these processes into the NJEMS framework. Additionally, through its service portal DEP Online, the NDJEP and CGI have been able to rapidly provide the ability for facilities and individuals within the state to meet the goals of NJ PACT, which seeks to build resiliency for the state by reducing greenhouse gas and other pollutant emissions, addressing the risks of sea level rise and promoting sustainability through recycling.

And today, the NJDEP and CGI are exploring ways to harness the power of Artificial Intelligence tools to allow the Department to realize true service value in exciting new ways and continue to lead through forward thinking and innovation.

RESULTS

CGI's recommendations and subsequent development and implementation of advanced IT initiatives at NJDEP have resulted in the following key successes:

- Today, NJEMS is used by more than **2,900** employees representing more than **25** program areas
- Through NJEMS nearly **1,000,000** facilities have been regulated, with more than **33 million** associated items
- DEP Online has received more than **1.3 million** online submissions through 400-plus services.
- The NJDEP has responded to more than **318,000** requests received through OPRATS

CGI's partnership with NJDEP demonstrates our ability to accurately assess client challenges and deliver results that achieve significant efficiencies, cost savings, and in many instances deliver solutions above and beyond the original project scope.

> "The CGI Team takes great effort to constantly discuss ideas to help NJDEP with specific technology needs and solutions, as well as long-range release and platform planning."
>
> **Jim Bridgewater**
> Assistant Director of Enterprise | Systems and Applications, NJDEP

ENGAGEMENT REFERENCES

New Jersey Department of Environmental Protection: Reference 1	
Name	Pete Tenebruso
Title	Chief Information Officer
Company	Division of Information Technology, NJDEP
Address	NJDEP Main Building 401 East State Street Trenton, NJ 08608
Phone Number	(609) 940-5899
Email Address	Peter.Tenebruso@dep.nj.gov

New Jersey Department of Environmental Protection: Reference 2	
Name	Jim Bridgewater
Title	Assistant Director of Enterprise Systems and Applications
Company	Division of Information Technology, NJDEP
Address	NJDEP Main Building 401 East State Street Trenton, NJ 08608
Phone Number	(609) 940-5539
Email Address	Jim.Bridgewater@dep.nj.gov

3.4.3 State of Louisiana Office of Community Development / Disaster Recovery Unit

Since March 2009, CGI has provided a full range of consulting services to the State of Louisiana's Office of Community Development – Disaster Recovery Unity (OCD/DRU) to support their recovery efforts after the historical destruction caused by Hurricanes Katrina and Rita. OCD/DRU was designated as Louisiana's lead agency in response to Hurricanes Katrina and Rita, receiving an initial $10.4B in funding through the HUD Community Development Block Grants – Disaster Recovery Program (CDBG-DR). Additionally, OCD/DRU received $1B in CDBG-DR funds to support recovery efforts from Hurricanes Gustav and Ike and administered the FEMA funded Hazard Mitigation Grant Program (HMGP).

ENGAGEMENT DESCRIPTION AND OBJECTIVES

The Louisiana Commissioner of Administration established the OCD/DRU in response to Hurricane Katrina, authorizing the Unit to orchestrate the State's relief efforts across multiple disaster recovery areas. The Road Home Housing Assistance Program (HAP) serves as the primary DR program. HAP is designed to compensate individual homeowners for residences moderately or severely damaged during Hurricanes Katrina and Rita. Additional program areas target the displacement of low-to-moderate income victims (Small Rental Property Program, and Low-Income Housing Tax Credits Program), and FEMA disaster mitigation funds for reconstruction (Hazard Mitigation Grant Program).

CGI was engaged by OCD/DRU in March 2009 to provide a range of consulting services to support the State's disaster recovery programs, including the provision of project management and oversight of core operations support services across all OCD/DRU's IT services.

The following are the overall objectives for the CGI engagement with the State of Louisiana OCD/DRU:

- Serve as OCD/DRU's primary IT expert to operate, improve, and otherwise manage all outsourced DR-related IT functions according to industry best practices and State and federal guidelines;
- Implement a program for continuous process improvement and provide active leadership to help ensure the quality and efficiency of IT services;
- Coordinate with non-IT stakeholders, including the State and program implementation contractors, to confirm that IT services are performing the right functions, and that priorities are correctly aligned across programs;
- Oversee subcontractor activities, including planning, issuing task orders, oversight and contract enforcement, deliverable review and approval, quality assurance and testing of software enhancements or fixes, and invoice review and pre-approval.

Overall, CGI is responsible for providing OCD/DRU with IT expertise, planning and implementation oversight across all aspects of the States disaster recovery initiatives, including its CDBG-DR initiatives, and to assist the State in achieving its ultimate goal of providing superior service to hurricane victims and other citizens of Louisiana in a manner that is efficient and produces cost savings over time.

CGI RECOMMENDATIONS

In March 2009, as part of OCD/DRU's transition to CGI as its primary IT consultant, CGI began performing an enterprise assessment of OCD/DRU's business needs and current state IT systems and infrastructure. CGI met with Subject Matter Experts (SME) from the Road Home Assistance Program (RHAP) to review the full range of organization, documentation and operating practices that were in use across the IT support functions prior to March 1, 2009. The assessment included performing an enterprise-level assessment of the quality and efficiency of IT services and processes, identifying continuous improvement opportunities and targeting specific areas that could be improved in the steady state support. CGI's understanding was that the Road Home IT organization had made limited use of established IT structures and best practices. A major focus of CGI's initial assessment determined what actions CGI would need to take to address critical management process gaps during the transition and build a best practice environment for supporting OCD/DRU's IT systems and infrastructure.

The assessment of OCD/DRU's Road Home Assistance Program included the facilitation of discovery sessions with SMEs from the State, OCD/DRU programs, program implementation contractors, IT subcontractors, and other project stakeholders related OCD/DRU's IT operations.

A summary of CGI's recommendations provided to OCD/DRU upon completion of CGI's initial assessment and analysis are as follows:

- **Initial assessment and analysis**: CGI's recommendation to conduct an initial enterprise assessment and analysis initiated a service-level dialogue with the implementation programs, provided a first step in documenting business requirements on application criticality, and provided needed alignment of IT support and program priorities. It also provided a basis for development-level process improvements, such as availability planning, systems engineering, backup requirements, and establishing priorities for ticket processing and setting recovery time objectives.
- **Change Management:** As part of the initial assessment and analysis phase of the OCD/DRU engagement, CGI recognized the lack of a standard process for collecting, assessing and reviewing changes to IT systems, infrastructure, and related processes. This represented a significant risk to delivering effective service during OCD/DRU's transition to CGI as its primary IT consultant. As a first step to addressing the current state situation, CGI deployed an interim change management process supported by a change request form and a change calendar. As a permanent solution, CGI recommended the establishment of a Change Control Board (CCB) at the Project Management Office (PMO) to review change requests for application enhancements, database modifications, and the development of new reports. CGI subsequently implemented a separate CCB to review modification requests to production operating environments, including hardware, application, database, reports, software releases and deployments.
- **Capacity Management:** With the limited focus that had been placed historically on this area, CGI recommended the development of a capacity management process that began with a comprehensive review of the current utilization levels of the Road Home servers and storage environments. This information provided an initial baseline and a documented capacity plan that was continuously updated based on system and data storage utilization trends and new business demand. Capacity and performance impact assessments were also established as a requirement in the Change and Release Management processes.
- **IT Service Measurement and Reporting:** The CGI Client Partnership Management Framework (CPMF) and detailed service management processes that are implemented across all our engagements, including OCD/DRU, rely on CGI's ability to collect high quality service data to

identify service and support issues and drive continuous improvement. CGI's initial assessment identified that there were limited systems management tools in place in many areas within the current state IT environment for managing service quality. CGI recommended that a detailed tools assessment be completed within each workgroup to identify minimum service measurement and reporting requirements, and then worked with the State to identify gaps and provide costs on specific deficiencies in current state tools. CGI also recommended establishing a standard set of KPIs for measuring service effectiveness and productivity.

- **Incident Management**: The weaknesses of OCD/DRU Incident Management process became evident during the early stages of CGI's initial assessment of current state IT systems and infrastructure. CGI needed to help ensure that all incidents would be identified and tracked and recommended the use of the help desk system for all IT support groups. The help desk team would work to separate incident ticket processing from the Service Request types, and re-work incident reporting data to provide better root cause definitions for downstream analysis and incident prevention. These actions would improve incident handling in the interim and provide a basis for moving forward in establishing improved root cause classification, a problem management process, ticket processing time objectives, and improved management and reporting capabilities. CGI also recommended that a well-documented Major Incident management process be adopted that outlines operational procedures to be followed when a major event occurs, such as the extended loss of a system. This process would include information such as criteria for defining a Major Incident and for engaging support Subject Matter Experts (SME) and key stakeholders from CGI, the Road Home Assistance Program, other program areas, and the State and its major vendors.
- **Request Fulfillment:** CGI recommended the implementation of a help desk tool to manage service requests for DR-related IT systems and infrastructure. The tool required that all user requests flow though the help desk with the exception of those requests handled by the Project Management Office (PMO) for software changes, enhancements and project work. CGI helped ensure that OCD/DRU reporting, and issue tracking requirements were considered prior to implementation, so that data collected through the process could be leveraged to support goals established in the Continuous Improvement Plan.
- **Problem Management:** Establishing best practices for problem management would require robust incident management processes as a foundation for success. As a follow-on activity under the Continuous Improvement Plan, CGI recommended separating incident management from problem management and documenting a set of new process for problem management, alongside well-defined roles, responsibilities, and specific procedures reporting and managing problems.

RESULTS

As a direct result of CGI's leadership, expertise, and the implementation of our recommendations to improve IT management and oversight practices, OCD/DRU has achieved the following milestones:

- Disbursement of more than **$8.9B** to rebuild homes through the Road Home Assistance Program (RHAP)

- Disbursement of more than **$400M** for the restoration of nearly **8,500** rental units through its Small Rental Property Program (SRPP)
- Disbursement over **$620M** to mitigate natural disaster risks to nearly **9,600** homes through the Hazard Mitigation Grant Program (HMGP)

ENGAGEMENT REFERENCES

State of Louisiana Office of Community Development/Disaster Recovery Unit (OCD/DRU): Reference 1	
Name	Tom Allsup
Title	State of LA Director of ARMs
Company	State of Louisiana Office of Technology Services for the benefit of the OCD/DRU
Address	PO Box 94095, Baton Rouge, LA 70804-9095
Phone Number	(225) 342-5284
Email Address	Tom.Allsup@la.gov

Louisiana Division of Administration: Reference 2	
Name	Brett Connison
Title	IT Statewide Director
Company	State of Louisiana Office of Technology Services for the benefit of the OCD/DRU
Address	PO Box 94095, Baton Rouge, LA 70804-9095
Phone Number	(225) 344-6314
Email Address	Brett.Connison@la.gov

3.4.4 State of New Jersey Department of Community Affairs

Although not applicable as a reference for this procurement, since June 2013, CGI has served as the primary IT consultant to the New Jersey Department of Community Affairs, Division of Disaster Recovery and Mitigation (DCA-DRM) in support of their ongoing disaster recovery efforts following the devastating impact of Superstorm Sandy. DCA-DRM has been designated the lead agency for implementing New Jersey's Action Plan to assist state residents, businesses, and communities in their recovery efforts in the aftermath of the storm. DCA-DRM has received over $11B in funding to date through the US Housing and Urban Development Agency (HUD) Community Development Block Grants – Disaster Recovery (CDBG-DR) Program, FEMA Mitigation Assistance Program (MAP), and the US Treasury American Rescue Plan Act (ARPA). This section highlights the successes achieved by DCA-DRM as a direct result of CGI's consultation.

ENGAGEMENT DESCRIPTION AND OBJECTIVES

DCA-DRM established the Disaster Recovery and Mitigation (DRM) focused on the administration of the Superstorm Sandy, Hurricane IDA, ARPA, and Mitigation Assistance recovery programs. CGI was engaged to provide a suite of services through the State Integrated Recovery Operations and Management Systems (SIROMS) project.

The following are the overall objectives for the CGI engagement:

- Provide sufficient depth of resources to support rapid implementation of New Jersey's Action plan and/or programs from other disaster recovery funding
- Provide back-office technologies and a mechanism by which the State of New Jersey could facilitate the distribution of recovery funds
- Create a gap solution within weeks of the engagement to begin immediately processing funds, while working on developing and implementing the longer-term solution
- Collaborate with partner agencies working with DRM to manage, track and report on the progress and delivery of recovery programs implemented by these agencies

Overall, CGI is responsible for providing DCA-DRM and its partners with a shared technology infrastructure, software, IT, financial and CDBG-DR services expertise to support the State in its disaster recovery operations. CGI supports systems that provide management and oversight capability, while supporting the State's compliance with State and Federal Regulations. The ultimate objective is to assist the State in delivering disaster relief services in a flexible, scalable and efficient manner.

CGI RECOMMENDATIONS

During the process of supporting DCA-DRM's disaster recovery objectives, CGI was asked to assess New Jersey's existing information and record keeping systems and provide recommendations that were targeted to help the State quickly deploy its CDBG-DR Programs to assist state residents impacted by Superstorm Sandy. CGI evaluated the existing solutions that supported the State's disaster recovery programs and provided an analysis on those data management systems and the reporting tools. CGI identified opportunities in many of the recovery programs and proposed improvements and targeted solutions identifying key timelines, resources and information system upgrades.

Specific recommendations were provided under the following categories:

- The State needed a Grants Management program that would bridge the gaps identified on existing programs and provide workflow solutions for a variety of programs.
- Enhanced reporting capabilities were required that would allow the State and Senior Management to answer multiple requests including auditors, OPRA and public facing information updates, and tracking overall progress.
- There was no integrated program to centralize the overall program direction including establishing the necessary data management systems
- Additional systems integrations with State, Banks, and other vendors' systems would result in reduced costs and increased efficiencies for the State.

RESULTS

CGI's expertise and the ability to implement CDBG-DR based programs have helped the State in delivering disaster relief services in a flexible, scalable and efficient manner. CGI has implemented a comprehensive suite of tools through SIROMS that have facilitated the successful management of the New Jersey State Recovery programs.

SIROMS functionality and initiatives include:

- **Funds Management**. CGI has developed a detailed accounting tool that allows DCA-DRM to centrally manage requests for Funds Distribution while accurately capturing both the required approvals and the supporting documentation. This set of financial management tools is still growing as DCA-DRM develops new needs for managing and tracking recovery funds. Seamless integration with the state's financial systems and with systems of other contractors working on recovery efforts have created cost efficiencies by reducing manual processes.
- **IT Program/Project Management**. CGI established Program Management and Oversight functions. Plans and processes were put in place to manage the engagement including the Program Management Plan, Change Management Plan, Program Tracking and Communication Plan, Issues and Risk Management Plan, Quality Assurance Plan, and the Software Development Lifecycle. Regular PMO meetings with all stakeholder groups has helped ensure that the status of all the initiatives were tracked and communicated across helping DCA-DRM savings in both cost and time by identifying cross program synergies.
- **Recovery Grant/Program Management**. SIROMS provides full life cycle program management for recovery grants, loans, and other programs that are managed by the State of New Jersey. SIROMS is customized to fit the needs of each program while taking advantage of the overlapping functions that most programs include. CGI has developed for SIROMS: public facing application intake systems, application randomization, eligibility determination and scoring, at a glance workflow status, document repository, complex grant award calculations, print screens that are used as part of legal grant signing agreements, status and history tracking to provide clear audit trail for all actions taken within the system, and direct integration with the Funds Management that allows the program staff to easily process and distribute funds.
- **Systems Development**. Acting on behalf of DCA-DRM, CGI has created and executed multiple full system development lifecycle project initiatives. These include various modules of SIROMS across multiple programs within DCA-DRM and the partner agencies.
- **Service Desk and Incident Management**. CGI has staffed and managed a Service Desk for reporting, tracking and resolving incidents, helping end users with various questions regarding the policies, systems, applications and reporting.
- **Quality Assurance, System and Integration Testing**. CGI has staffed and managed Quality Assurance, Systems and Integration Testing. System and Integration testing is an integral step for every project work stream. Test Plans, Test Tracking and Results Report as well as User Acceptance frameworks have been established and utilized for each system development initiative.

- **SQL Database Management**. All SIROMS systems are built on an SQL database platform which creates consistency for reporting needs.
- **Data Warehouse Management/Reporting**. CGI has staffed and managed a Data Warehouse Team and a Reporting Team to provide ad hoc and scheduled reports to DCA-DRM and Program Management and staff. An integrated data warehouse with all the agencies working on the recovery efforts provide consolidated information to multiple transparency portals including the Governor's Office of Recovery and Rebuilding (GORR), and the Office of the Comptroller.
- **Business Intelligence Reporting**. CGI has staffed and managed a Business Intelligence Reporting team. Providing statistical analysis and forecasting methodologies has helped the State identify bottlenecks in operations, provide estimates on program completion, plan for resource allocations and project for financial disbursements through the life of the programs.
- **Enterprise Content Management Server** (ECM) integration has helped DCA-DRM by providing a single source of record for any documentation that is associated with the recovery efforts
- **Managed Services/Hosting**. CGI hosts all of the SIROMS components in our secured cloud environment which provide end to end grant management solution to DCA-DRM.
- **IT Disaster Recovery Planning and Testing**. The Infrastructure Team is responsible for Disaster Recovery Planning and Testing.
- **Geospatial Information Services**. CGI has built an ESRI ARC-GIS enabled web portal for DCA-DRM.
- **Quarterly Performance Report (QPR)**. CGI's SIROMS solution facilitates the centralized collection and aggregation of this data to help ensure smooth report generation and entry into the federal systems.

Some of the key successes of CGI's partnership with the State of New Jersey for CDBG-DR efforts include:

- Managed over **$11 billion** in federal and state funds
- Over **$6.6 billion** in recovery funds disbursed through SIROMS implementation (to date)
- Facilitated delivery of over 66,000 checks to New Jersey residents
- Identified over 4,600 Accounts Receivable totaling approximately $146 million and collected over $60 million of the outstanding debt
- Captured over $52 million in Program Income and reinvested over $47 million into existing programs
- Recovered over $8.5 million in grant funding related to fraud payments
- **25,906** Homeowners served through the program
- **11,346** renters served through SIROMS Systems
- NJ Government has successfully submitted **57 QPRs** to date on time and with no comments
- CGI has assisted DCA-DRM successfully pass multiple audits from multiple organizations including HUD and HUD-OIG
- More than **170** canned reports delivered on automated schedules

CGI's recommendations and technology/governance implementations have had a significant impact for the State of New Jersey as they help thousands of people recover from a historic tragedy. DRM's recovery programs and initiatives have been able to move forward quickly helping businesses create new jobs, communities remove dangerous structures and replace them with park and green spaces, people moving out of their temporary shelters and move back into secure homes.

ENGAGEMENT REFERENCES

New Jersey Department of Community Affairs: Reference 1	
Name	James Shuster
Title	Deputy Director / Chief Information Officer
Company	New Jersey Department of Community Affairs
Address	101 S Broad St, Trenton, NJ 08608
Phone Number	(609) 930-1488
Email Address	James.Shuster@dca.nj.gov

New Jersey Department of Community Affairs: Reference 2	
Name	Parth Sampath
Title	PMO Manager
Company	New Jersey Department of Community Affairs
Address	101 S Broad St, Trenton, NJ 08608
Phone Number	(609) 913-4268
Email Address	Parth.Sampath@dca.nj.gov

4 Data Security Requirements

4.1 Security Plan

A detailed security plan has been attached in Appendix D.

4.2 Information Security Program Management

At CGI, the overall accountability for security management is undertaken by the role of Chief Security Officer that is assigned at the SVP level with direct report to the CLO (Chief Legal Officer). Reporting to the Chier Security Officer is a dedicated team of Security Partners who are responsible for creating the security framework and for disseminating information to project teams like SIROMS. This team holds weekly meetings focused on current security issues to help ensure that all project team members are up to date on the latest vulnerabilities and security-related issues. During these meetings, participants review any new or ongoing vulnerabilities, assess potential risks, and discuss ways to strengthen the organization's security posture. This collaborative approach allows the SIROMS project team to promptly address security challenges, share insights, and coordinate actions to safeguard critical systems and data. Regular security discussions also reinforce a proactive security culture, helping the organization stay prepared for evolving threats.

CGI has developed and operates a Security Program supported by a comprehensive Enterprise Security Management Framework (ESMF). Inspired by industry's best practices, ESMF is designed to adapt for CGI security needs to effectively support CGI operations. The ESMF supports responses to client requests for information, proposals and external audits related to security, and it also supports the CGI's ISO 27001 certificates and other industry recognized security standards. The ESMF is based in two fundamental elements: a risk-based methodology and a business-focused approach that allows managing security and business continuity in alignment with CGI's risk tolerance fostering a risk sensitive culture. The framework sets the security baseline to protect CGI and client operations while allowing continuous improvement for security program evolution. It establishes an efficient governance security model, clear and formal security processes and a complete set of policies supported by standards to manage security and business continuity effectively.

In preparation for external certification audits, a compliance audit is conducted by the Internal Audit team upon request. This may include new certifications, renewal of existing certifications, and/or changes in scope, etc. The Internal Audit function is an independent internal team accountable to the CGI Audit and Risk Management Committee.

CGI employs a robust internal security framework that includes real-time alerts to notify users of any current vulnerabilities within the environment. This proactive approach to security is reinforced by continuous system scanning and monitoring. Key tools include Trend Micro for endpoint protection, CrowdStrike for advanced threat detection, IPcenter for comprehensive system monitoring, and Nessus for vulnerability assessments. These integrated solutions help maintain a secure infrastructure, enabling timely responses to potential threats and enhancing overall system resilience.

4.3 Compliance

CGI will provide DCA-DRM with the contact information for the individuals responsible for maintaining our certification compliance with in 10 days of the start of the contract.

CGI will continue to perform security assessments through out the solution development process. For details on the policies and procedures please see section 4.29.

The SIROMS SaaS will maintain a NIST 800-53 rev. 5 or above compliance. A third party can and will, at DCA-DRM's request and authorization, confirm this compliance. The infrastructure upon which the SaaS is built is certified by AWS to meet FedRAMP moderate compliance.

4.4 Personnel Security

Workforce security policies and procedures are listed in sections 3.2 and 3.3 of the Security Plan found in Appendix D.

4.5 Security Awareness and Training

Workforce security policies and procedures are listed in sections 3.2 and 3.3 of the Security Plan found in Appendix D.

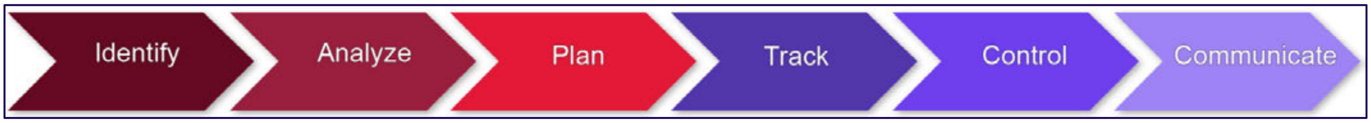
4.6 Risk Management

To manage risks and issues for SIROMS, we will utilize the CGI risk and issue management framework. The framework follows the risk management best practices outlined by the PMBOK. Unless requested to do otherwise, CGI will log issues and risks in the weekly status report and risks and issues will be reported on in the weekly Management Meeting.

The CGI team will monitor and manage project risks and issues using an iterative risk and issue management approach consisting of the following risk management practices:

- **Identify:** The CGI team will document risks and issues based on events that might enhance, prevent, degrade, or delay the achievement of project objectives. This is initially completed during the inception of the project with client stakeholder engagement and input, and it is regularly updated going forward for the entirety of the project.
- **Assess and Analyze:** The project team will consider the causes and sources of potential risks and issues, their positive and negative consequences, and the probability of occurrence. Using an assessment instrument, risks and issues are then quantitatively categorized and prioritized for monitoring.
- **Respond and Plan**: Once risks and issues are identified and prioritized, the project team will discuss, plan, and implement specific proactive mitigation actions for each risk.
- **Monitor and Control**: The project manager will monitor risk and issue responses via a risk and issue log. Examples of monitoring and control include:
  - Detecting changes in the external and internal environment, including changes to the risk itself
  - Confirming that the risk controls and mitigation activities are effective in both design and operation
- **Communicate**: the project manager will minimally communicate regarding risks and issues via the weekly status report and weekly management meeting. The project manager and/or risk owner may communicate more frequently as they work to mitigate the risk or resolve the issue.

Exhibit 19 - Risk and Issue Management Practice



Key details to be documented via the weekly status report include:

Risks:

- Type of Risk
- Severity
- New or existing
- Title and Description
- Mitigation Plan/Current Status

Issues:

- Type of Issue
- Severity
- Title and Description
- Date Added
- Target Resolution Date
- Current Status

4.7 Privacy

All data in the SIROMS SaaS is exclusive owned by the state of New Jersey and data used in the SIROMS SaaS is governed by New Jersey compliance standards. CGI has divided all SIROMS data into PII and non-PII data, with all PII encrypted at rest and all data encrypted in transit using HTTPS with a TLS level of at least 1.2.

SIROMS does not currently utilize any health or payment data therefore HIPPA, and PCI DSS do not apply to the system. CGI will continue comply with IRS Publication 1075, *New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11- 44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4*.

CGI agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. We will seek to ensure that State Data is secured and encrypted during transmission or at rest.

Data will only be transmitted to third parties with expressed written consent of DCA-DRM. All data is maintained in the AWS GovCloud infrastructure, with data residing only in the United States. Because AWS is a cloud infrastructure, it is not possible to directly transfer SIROMS data to any portable device, including USB devices. All CGI personnel are trained not transfer such data from their local laptops, which encrypt a portable media attached to them.

In the event of a data breach, CGI will notify DCA-DRM within 24 hours of detecting the breach and a single CGI employee will be designated as single point of contact for DCA-DRM. Unless prohibited by an applicable statute or state order, CGI will not notify the public of such a breach until the State gives permission for such disclosure.

All state data is backed up and in the event of the termination of the contract, all data will be transferred back to the state as designated in the contract.

CGI will work with the SCM to define a schedule to transfer data to the state. At the termination of the contract, after the final data transfer, CGI will render all system data unreadable.

In the unlikely event of the loss of data, CGI will work with the SCM to recover the data from the system back ups as quickly as possible.

4.8 Asset Management

CGI understands that hardware assets have a multifaceted lifecycle. Managing the hardware asset is included in CGI's organizational practice to help ensure that all Hardware IT Assets are aligned with organization's objectives. CGI's IT Asset Management (ITAM) consists of a framework and corresponding processes that strategically track and manage all financial, physical, licensing and contractual aspects of IT assets throughout their life cycle. CGI ITAM framework has the following functions:

- Asset lifecycle management - Ability to capture the asset lifecycle data from requisitioning to assignment of assets, expiry date and asset disposals.
- Maintain Asset Repository data of workstations.
- Identify and track changes in the location of every asset, track asset statuses and user information.
- Control traceability of assets for better administration.

In addition to the use of the ITAM framework CGI mandates every partner to adhere to Security and Acceptable use policy. CGI Security and Acceptable sue policy outlines the following policies for Asset Management:

- CGI and client's assets and resources are to be accessed by authorized users only.
- Passwords are required when accessing a CGI computer account to protect CGI and client information. Passwords must be changed on a regular basis and adhere to CGI password security requirements as documented in the Access and Privilege Management Standard Passwords may not be shared or used by any other individuals.
- CGI computers must have active anti-virus and personal computer firewall protection that is regularly updated. CGI laptop computers must be encrypted.
- CGI secures authorized remote connection to connect to CGI networks.

4.9 Security Categorization

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.10 Media Protection

CGI's Data Privacy policy establishes procedures to help ensure data and information, in all forms and mediums, are protected throughout its lifecycle and based on the sensitivity and the impact of data breach to the client.

SIROMS data will be maintained on various types of AWS storage including relational databases, quick access AWS S3 file storage, and longer-term AWS Glacier storage for regulatory retention. All discrete data used by the SIROMS application is stored within the relational database and is encrypted while at rest. The SIROMS application accesses the relational database through APIs using encrypted endpoints thus ensuring that the data is also encrypted during transport. Non-discrete data, such as document attachments, are stored within an enterprise content management system which obfuscates the document before placing it on the AWS file system. The document cannot be properly rendered without going back through the enterprise content management system.

CGI's Data Privacy policy also establishes procedures for generating a Data Protection Inventory for every CGI engagement with a client where sensitive data is involved. This inventory is maintained throughout the lifecycle of the engagement and describes where sensitive data is located, how it is processed, and the safeguards taken to protect it.

All SIROMS public-facing and internal application endpoints are protected by encrypted endpoints. These endpoints use certificates from industry standard Certificate Authorities, include 256-bit encryption keys, and use industry best-practices encryption algorithms.

As the SIROMS solution is a SaaS, directly connecting portable media to it is not a concern due to the limited access to secure AWS facilities. To mitigate the risk of users connecting to the VPC and copying data to a portable device, CGI enforces that all portable media are encrypted.

In conjunction with State of NJ regulatory requirements and CGI data retention requirements, SIROMS will use AWS S3 storage for daily backups and monthly pushes to AWS Glacier long-term storage. Data more than a year old will only be available from AWS Glacier backups. Any client data beyond the regulatory retention period will be deleted from AWS Glacier on a monthly basis.

Sanitization procedures for deleted files from all AWS storage media is handled by AWS. The AWS GovCloud has automated protocols for cleansing deleted files.

4.11 Cryptographic Protections

CGI uses cryptographic safeguards to protect all client data used within the SIROMS application.

Certificate and cryptographic key management are handled by CGI Security Operations Center (SOC) and follows strict protocols. Only industry standard Certificate Authorities are used to validate public certificates and 256-bit public/private keys. Industry standard cryptographic algorithms of Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are both employed to protect SIROMS data in transit and at rest.

Transport Layer Security (TLS version 1.2) encryption and SSL certificates provide robust protections for data in transit. TLS is an industry-standard encryption protocol that secures data by encrypting it during transmission between servers and clients, helping to prevent unauthorized access or interception. The use of SSL certificates, which authenticate and establish secure HTTPS connections, further helps ensure that data is protected by validating the server's identity and enabling encrypted communication.

The Transparent Data Encryption (TDE) is enabled for the SIROMS Application Database to comply with the State of New Jersey's Security Policies and Requirements. The TDE is at the Database File level, so application data, log, and backup files are encrypted using TDE, which require encryption certificates/keys to migrate and restore the database on another Database Server. SIROMS Application Database cannot be restored/attached to another server without the encryption key/certificate.

4.12 Access Management

CGI follows both Project Management Body of Knowledge (PMBOK) and ISO 27001 procedures in following the principle of granting least privileged permission to accomplish required functions and access to organizational assets. In fact, as of October 2024, local admin privilege has been removed by default for all CGI laptops requiring an administrative process to acquire such privilege.

Authorization to organization assets, including the SIROMS SaaS are controlled by the principle of role-based access control (RBAC). Periodic reviews of access authorizations and controls are conducted by the SIROMS infrastructure team as well the leaders of various SIROMS project teams, especially when a team member is added or transferred to different function on the SIROMS team. The SIROMS infrastructure team removes access to all CGI and NJ DCA employees when their manager informs the team they have transitioned to another role. All client tickets to remove access are tracked via Helpdesk tickets with the status tracked by completion of the ticket.

Duties are segregated amongst the SIROMS infrastructure staff. There are separate roles and access for database administrator, network administrator, and server administrator.

CGI conducts periodic reviews of access authorizations and controls to help ensure that access privileges align with current roles and responsibilities. As part of this process, the team reviews LDAP (Lightweight Directory Access Protocol) account statuses to verify that users have appropriate permissions and that any inactive or outdated accounts are promptly identified and deactivated. This regular assessment helps maintain a secure environment by ensuring that only authorized personnel have access to sensitive systems and data, reducing the risk of unauthorized access. By routinely auditing and updating LDAP account statuses, the organization upholds strong access control measures and aligns with best practices for data security.

4.13 Identity and Authentication

Section 3.3 of the 2024 NJ SIROMS Security Plan describes how the identity, authentication and the authorization required to access resources of the SIROMS SaaS are implemented.

CGI personnel supporting the SIROMS project require two-factor authentication to access the AWS hosting environment. In addition, AWS access controls are used to determine which AWS resources a user is permitted to use.

4.14 Remote Access

Section 3.7 of the Security Plan (Appendix D) describes how remote access to the actual physical infrastructure upon which the SIROMS SaaS is built is tightly controlled by AWS and how CGI has implemented technical security controls.

Section 3.2 of the same security plan, under Workforce security, details how user training for remote access is administered.

Robust security measures are in place in order to remotely access CGIs internal infrastructure, including mandatory multi-factor authentication (MFA) and IP whitelisting. MFA adds an extra layer of protection by requiring users to verify their identity through multiple methods, ensuring that only authorized individuals can gain entry. Additionally, IP whitelisting limits access to trusted network addresses, further safeguarding critical systems from unauthorized access. Users also participate in periodic security training to stay informed about the latest security risks and best practices. This training covers topics like phishing, secure password management, and data protection, reinforcing a security-aware culture and reducing the risk of human error. Through these combined efforts, the organization promotes a secure and resilient environment.

CGI will collaborate with NJ DCA to help ensure that State-owned data and IT resources are accessed and used in accordance with all State defined usage restrictions and configuration/connection requirements.

4.15 Security Engineering and Architecture

Defense in depth with 24x7x365 Security Operation Center (SOC) monitoring is implemented in a classic shared responsibility model with the SIROMS infrastructure team maintaining EC2 security, including initial hardening to NIST standards and monthly patching. A different division of CGI maintains the SOC with additional monitoring, including IT Operations Management (ITOM) and AWS monitoring tools. The SOC also performs monthly Nessus reports on vulnerabilities, which are shared with the SIROMS infrastructure team to remediate.

The SIROMS SaaS is divided into a three-tier model and all ingress and egress is controlled and monitored by redundant Next-gen firewalls. All security boundaries in SIROMS SaaS are logical in the AWS public cloud. The infrastructure upon which the SIROMS SaaS is built maintains a FedRAMP moderate compliance, which mandates technical, administrative and physical controls. Each server in the AWS cloud is synchronized to with its domain controller and all CGI developer laptops are synchronized to the CGI domain controller. CGI tailors its security controls by first conducting a comprehensive risk assessment to identify specific threats and vulnerabilities relevant to its operations. By aligning security measures with business objectives and regulatory requirements, CGI customizes access controls based on user roles and integrates security solutions that fit its technology environment, ensuring that security enhances operational efficiency rather than disrupts it.

The SIROMS software development lifecycle is predicated on the Project Management Body of Knowledge best practices. These practices help CGI maintain a secure posture for the entire lifecycle of software development. Security started in the requirements phase with SIROMS and is incorporated not only in the SIROMS technical infrastructure but also the application design and implementation phases. Production monitoring by the SIROMS infrastructure team and CGI SOC provides a continuous security posture in the current post-production phase.

The SIROMS SaaS undergoes routine 3rd party penetration testing (PEN) whereby hackers attempt to breach the system through both public access (as an end user) and internal access as a SIROMS project team member. Hackers attempt to obtain elevated privileges and acquire more application and system access than what is normally prescribed.

The SIROMS SaaS has undergone dozens of Disaster Recovery scenarios ensuring that the entire system fails-safe with a minimal recovery point objective.

4.16 Configuration Management

Configuration Management is described in detail within section 3.9 of the 2024 NJ SIROMS Security Plan. Details of hardening systems can be found within section 3.5.2 and least privilege access details can be found within section 3.3.

4.17 Endpoint Security

All CGI laptop endpoints are protected with anti-malware software and hard drives are encrypted at rest. Asset management software runs to help ensure only CGI sanctioned programs installed. Any portable storage devices used by CGI laptops are also encrypted at rest.

CGI's Asset Management policy extends to our SIROMS SaaS ensuring that all endpoint devices, physical or logical, are properly cataloged and accurately maintained. Because AWS GovCloud maintains FedRAMP moderate compliance, it too must maintain an accurate inventory of physical and logical devices.

CGI's Data Privacy policy applies to all phases of the project lifecycle. As part of the Data Processing Inventory, all endpoints that either store or in some way touch sensitive data must be part of that inventory. Specifically, as part of the SIROMS SaaS, encryption protects all data while at rest within the database endpoint. Web servers hosting the SIROMS web application are protecting sensitive data in transit through secure Certificates using 256-bit encrypted public/private keys. Furthermore, the SIROMS application endpoint uses identity management to permit only authenticated users and role-based access control to help ensure sensitive data is viewable to only proper users.

Software updates and patching are handled by the SIROMS SaaS infrastructure team. We follow Microsoft patching schedules and apply operating system patches first to our Test environment and then a week later on the Production environment. Operating system supportability is ultimately controlled by AWS public cloud based on the type of EC2 templates they permit. All SIROMS SaaS instances have viable operation system versions through the lifetime of this contract. The SIROMS infrastructure team monitors software vendor sites on a monthly basis. Any critical security alerts from software vendors come via email through maintenance support contracts.

As mentioned previously, SIROMS data is protected both at rest using database encryption and in transit through secure Certificates using public/private keys. All public endpoints use Transport Layer Security (TLS) version 1.2 or higher. Only required ports are opened that are required to maintain application functionality.

The CGI Security Operations Center (SOC) maintains all firewalls and provides continuous monitoring capability for network intrusion including daily log monitoring. Blacklisting and Whitelisting are used to control access to the SIROMS SaaS from various IP ranges. The CGI SaaS also uses AWS anti-malware services on all its EC2 instances.

Specific baseline configurations for CGI assets are established based on requirements and CGI policies and standards. CGI considers these documents as proprietary and confidential. As such, we can:

- Host a Teams meeting to walk the client through our policies and procedures,

- Send them a copy of our Security Baseline Overview which provides a detailed overview of CGI's Security Program and Policies or
- Make printed copies and bring them to the client's site to review in person at the client's expense.

4.18 ICS/SCADA/OT Security

The SIROMS SaaS is built within the AWS Government Cloud. AWS maintains and secures ICS/SCAD/OT assets and has developed policies that meet the FedRAMP moderate regulatory compliance level. Any further security concerns are outside of the scope of the SIROMS SaaS.

4.19 Internet of Things Security

The SIROMS SaaS is comprised of standard Internet web application components such as web, application, and database servers. It does not use physical devices in the form of sensors actuators, or other embedded electronic devices to exchange data. Any further security concerns are outside of the scope of the SIROMS SaaS.

4.20 Mobile Device Security

All mobile devices connecting to CGI networks are encrypted and centrally managed. If devices are out of date in their patch level, their access to CGI networks is denied until they have been updated. Only approved CGI mobile applications can be used to access CGI network and data. Initial training of all CGI employees includes safety and security training of mobile devices.

Only CGI certified mobile devices that meet CGI security standards are authorized to connect to the CGI email system. The CGI endpoint security standard and its ES8 mobile security control enforces security on all mobile devices connected to the CGI systems. Any device if connected to the CGI corporate email system will be deemed a company device in order not to compromise corporate security and to protect both CGI and client data.

CGI may perform remote operations on these devices including the enforcement of device encryption and more specifically in the even of loss or left of any such device or if the partner leaves the company, wiping of the entire device data should occur to avoid a situation where corporate security would be compromised. All applications that can access the CGI network are managed using a CGI profile that is installed on the device. The CGI profile protects cross profile data transfer.

4.21 Network Security

The SIROMS SaaS is built upon the AWS FedRAMP moderate compliance Platform as a Service (PaaS), which includes limited network access points and restricts split tunneling. All networks in the SIROMS SaaS and CGI's network are segmented with intrusion detection system (IDS) monitoring and maintains an extensive DDoS offering known as AWS Shield. The SIROMS infrastructure team uses AWS security groups providing defense-in-depth access to infrastructure and application resources. The SIROMS SaaS also uses Transparent Data Encryption as well as whole disk encryption at rest and only supports HTTPS at a transport layer security (TLS) level of 1.2 or higher. All ingress and egress is controlled by redundant Next Gen firewalls using access control lists.

4.22 Cloud Security

Controls necessary to protect sensitive data in public cloud environments are implemented within the SIROMS SaaS. CGI is using AWS's GovCloud environment to host the SIROMS SaaS. AWS maintains a strict compliance regiment and is trusted to continue to maintain that compliance by multiple federal agencies. CGI maintains a list of trusted vendors, including cloud service providers. CGI partners with AWS to securely bring their cloud offerings to CGI customers. RACI models for responsibilities by CGI entities have been ratified along with AWS published responsibilities. CGI has divided all data in SIROMS SaaS as either personal identification information or public and all data is protected with encryption at rest and in transit using already mentioned cryptographic algorithms and standards.

CGI will seek to ensure that the design, configuration, and implementation of cloud-based applications, infrastructure, and system-to-system interfaces are carried out in alignment with the mutually agreed-upon service, security, and capacity-level expectations.

4.23 Change Management

The Change Control Management Plan, developed in partnership with DCA-DRM, identifies workflow processes required to implement changes across the SIROMS environment. In addition, it identifies managed and controlled work products and defines Change Control Management responsibilities for managing and controlling them.

A Change Request module was created within the SIROMS suite of applications that is used to track the progress of an individual change from its initial conception, through its design, development, testing, and production deployment. This tool allows for accurate record keeping of the progress and approvals of all changes to the system. Changes are not developed until they have been approved by the appropriate stakeholders or writing notification to proceed has been granted. None of these changes are deployed to the production system until an email approval of the change is sent from DCA-DRM.

OpentText BPM and the APIs developed for SIROMS are built on frameworks that require that user roles are specified for all custom list and action access within them to help ensure that access roles are specified. The actions and custom list access that should be available to specific roles are delineated in a user access matrix that is provided as part of the documentation for each change request. CGI's quality control team tests all changes to the user access matrix as part of the testing process for any change and any deviations between the matrix and actual system function are returned to the development team as bugs to be corrected before user testing can start. As part of the production deployment process, CGI verifies the accuracy of the availability of all actions that have been updated as part of any changes that are being deployed.

4.24 Maintenance

A combination of the SIROMS program and infrastructure teams are responsible for providing routine application and infrastructure maintenance. Operating system security patches are automatically deployed and manually run twice a month. SIROMS SaaS third party software components are monitored routinely for security patches. SIROMS application maintenance releases are designed, implemented, tested, and deployed on an as-needed basis in conjunction with both CGI and NJ DCA.

All technology assets used by the SIROMS SaaS are virtual. AWS has the responsibility of vetting, monitoring and escorting vendors to maintain their physical hardware while maintaining confidentiality, integrity, and availability of all computing assets.

4.25 Threat Management

CGI’s Security Management team has defined the governance around threat analysis, awareness, mitigation, and if necessary, remediation. CGI Security Policies outline several sources from which threat intelligence is acquired. CGI considers these documents as proprietary and confidential. As such we can:

- Host a Teams meeting to walk the client through our policies and procedures
- Send them a copy of our Security Baseline Overview which provides a detailed overview of CGI's Security Program and Policies or
- Make printed copies and bring them to the client’s site to review in person at the client’s expense.

4.26 Vulnerability and Patch Management

All of the servers that host the SIROMS SaaS run the Windows 2019 or 2022 OS. Microsoft releases patches for these servers every second Tuesday of the month. A non-cloud test and development environment that includes similar functionality as the SIROMS infrastructure is patched the weekend after patch Tuesday as an initial testbed for the patches. The production and disaster recovery environments are patched one week after the UAT environment.

There are both pre-patching and post patching reports that are generated by AWS Systems Manager on the state of patching of each server to confirm success/failure. The SIROMS infrastructure team uses these reports and Nessus reports to perform our due diligence and confirm that the SIROMS infrastructure is safe and secure. As contractually required, CGI will employ third parties (A-LIGN is an approved vendor often used by CGI for penetration testing) to conduct penetration test as contractually required.

4.27 Continuous Monitoring

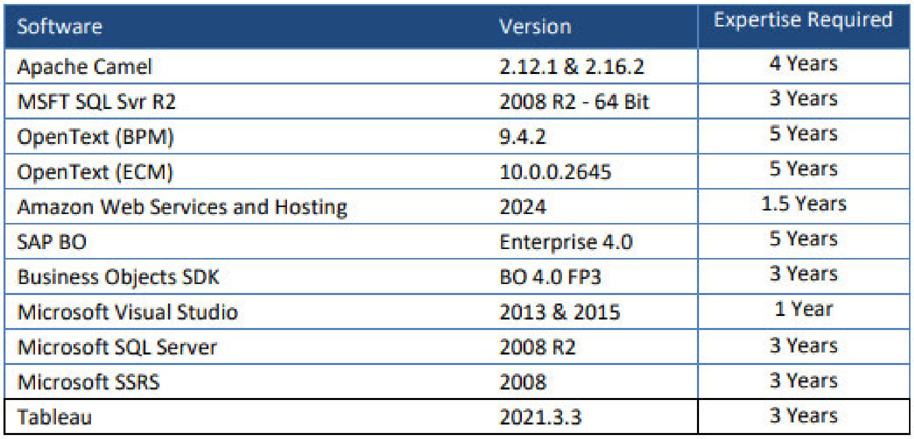
CGI has a dedicated Global Security Operations Center (GSOC) that provides ongoing security monitoring, incident management, threat intelligence, threat management and forensic investigation. The GSOC monitors CGI’s network and critical assets on a 24x7 basis in geographies where CGI operates. The GSOC also provides ongoing proactive testing of CGI’s network to evaluate if controls perform as expected against the current cyber threats.

The SIROMS SaaS is monitored by a separate SOC 7x24x365 using their own set of tools, including Next-gen firewalls and web application firewalls (WAF). Security logs are routinely monitored for relevant information and tamper detection. CGI’s Security policies define investigation procedures including notification protocols if a security incident occurs.

4.28 Software Environment

Since CGI has been hosting and developing the SIROMS suite of applications since 2013, the CGI team will easily be able to meet and exceed the expertise requirements specified in the table below. For specific details on the skill sets of our CGI Partners, please see the resumes in Appendix A.

CGI can procure new software required for SIROMS within 30 days from the point of contact with the software vendor.



Software	Version	Expertise Required
Apache Camel	2.12.1 & 2.16.2	4 Years
MSFT SQL Svr R2	2008 R2 - 64 Bit	3 Years
OpenText (BPM)	9.4.2	5 Years
OpenText (ECM)	10.0.0.2645	5 Years
Amazon Web Services and Hosting	2024	1.5 Years
SAP BO	Enterprise 4.0	5 Years
Business Objects SDK	BO 4.0 FP3	3 Years
Microsoft Visual Studio	2013 & 2015	1 Year
Microsoft SQL Server	2008 R2	3 Years
Microsoft SSRS	2008	3 Years
Tableau	2021.3.3	3 Years

4.29 System Development and Acquisition

CGI recognizes the impact that allowing insecure application code into the SIROMS system could have on DCA-DRM. An unmitigated vulnerability in the system could cause the loss of personal information that program applicants have entrusted that state to use responsibly or system outage that could delay the delivery of services to DCA-DRM's clients. To prevent these negative outcomes, CGI implements the following policies:

- When any change to the application code is made, the developer reviews the code using the following check list:
  - Confirm that any HTTP request or response is restricted to authenticated users and that any necessary role and attribute filtering is checked at the start of the request. If the request is valid for unauthenticated users, ensure no sensitive data or processes are exposed by it.
  - Confirm that role and attribute checks are done against data structures that couldn't have been modified by an untrusted source.
  - Confirm that all data integrity validations are performed by code executed on a trusted server. Duplicate checks can be performed on the client machine to improve user experience, but this is not a substitute for server-side checks.
  - All user input should be sanitized before it is processed to prevent common forms, HTML, code and SQL injection.
  - Avoid concatenation of SQL strings to prevent SQL injection. If concatenation is necessary to create dynamic code, evaluate how all user input is handled to help ensure that SQL injection can't occur.
  - All user authentications should utilize the existing authentication libraries.
  - Input validations should be performed before any database updates are made and the process should exit before updates are triggered.
  - If a system exception is encountered, confirm that all updates made as part of the request are rolled back and that the error is logged with as much detail as possible.

- Code is periodically reviewed by senior developers to confirm that the check list above is being followed.
- The SIROMS project uses 3 environments, Production, Test, and Staging. The Production servers and databases are kept in a separate network from Test and Staging. Access between the Production and Test networks is highly restricted. The segregation between these 2 regions prevents accidental access of information of production data from a test application and allows for varying restriction of user access between the 2 environments.
- As part of all change requests, regression testing of the affected modules access matrix is performed to prevent the introduction of an access vulnerability.
- The application source code is stored in a Subversion version control repository. This repository is located within a secure subnetwork in CGI's network, requiring users to have 2 factor VPN access to CGI's network and be granted access to the subnetwork. In addition to this access to the repository is restricted by an additional username and password that is only granted to active members of the SIROMS development team. CGI will not share the source code from SIROMS outside of the project without the consent of DCA-DRM.
- Guidelines are issued and periodically updated by CGI to all employees on secure coding practices.

These guidelines cover strategies for dealing with authentication, session management, code injection, SQL injection, cross site scripting, redirects and forwards, cross site request forgery, and data loss prevention.

4.30 Project and Resource Management

CGI employs a hybrid agile approach to the Software Development Life Cycle (SDLC), with a focus on deep collaboration with program management and staff. This is an approach that CGI and DCA have refined together over the course of the project. It provides a release cadence that produces system updates as quickly as possible while allowing the requesting users the opportunity to provide feedback on the changes so that they can be fine tuned before they are moved to the production environment. This release frequency also allows for off cycle changes to be defined, developed, tested and deployed during the release as necessary. With any change to the SIROMS application, security impacts are assessed at several phases of the life cycle:

- High Level Design – Once the basic function requirements of a change are understood, these requirements are given to the application development manager for a feasibility review. Part of this review includes determining if there are any concerns inherent in the changes being proposed. Examples of this would include the need to allow the system to permit an unauthenticated request or the need to interface with a third party. If a security issue with the changes is identified, CGI will send the requirements to its security specialists for review. CGI will recommend ways to mitigate the risks involved in the change, notify DCA-DRM of any potential risks that remain, and may recommend against the change if they feel that there are significant risks that can't be mitigated.
- Detailed Design – As part of the detailed design process, CGI works closely with DCA-DRM to help ensure that access requirements for all actions that are being modified are clearly defined. The changes are reviewed to confirm that the information and controls in the system are only available to the appropriate system users. A user access matrix is developed as part of the detailed design of these changes to help ensure that user access is clearly delineated for all system resources.
- Development – As part of the development process, CGI performs code reviews and has developers follow a checklist or security items to prevent the introduction of insecure code into the application. More details on this process can be found in section 4.29.
- Test – As part of the testing process, CGI validates all changes against the user access matrix for the modification to verify that the access allowed is correct.
- Deployment – After changes are deployed to production, access changes to pages and controls are verified in the production environment to help ensure that they are configured correctly.

4.31 Capacity and Performance Management

The SIROMS infrastructure team monitors the performance of the SIROMS SaaS to maintain availability, quality, and adequate performance. The SIROMS SaaS is built on the AWS cloud environment, which maintains an extensive DDoS offering known as AWS Shield, which CGI is utilizing for the SIROMS SaaS. Monthly reports, using AWS tools, such as Cloud Watch, AWS config and Cloud Trail as well using AWS SIEM will be utilized to monitor the performance of the SIROMS SaaS.

4.32 Third Party Management

CGI Inc., its subsidiaries and affiliates (collectively, "CGI") is committed to unyielding integrity and high standards of business conduct in everything it does, including in its dealings with its business partners (i.e., any party with whom CGI does business including, but not limited to, primes, subcontractors, independent contractors, consultants, distributors, licensees, suppliers, or other agents, collectively "CGI Third Parties").

To help CGI Third Parties understand the CGI commitment to unyielding integrity and the standards of business conduct, CGI has prepared this Third-Party Code of Ethics (this "Code"). CGI is required to maintain compliance with various acts, statutes, and regulations governing activities in the jurisdictions in which it carries on business and expects CGI Third Parties to do likewise. CGI only does business with individuals and companies that act in accordance with applicable legal requirements. CGI Third Parties are expected both to comply with their contractual obligations to CGI and to adhere to standards of ethics and business conduct consistent with this Code. A commitment to full compliance with these standards is the foundation of a mutually beneficial business relationship with CGI.

CGI Third Parties also shall maintain the confidential information of CGI and its clients by not transferring, publishing, using, reproducing, or disclosing it without the prior written permission of CGI. CGI Third Parties shall comply with all applicable privacy regulations and standards (including standards imposed by CGI's clients by contract or otherwise) to the extent that confidential information contains personally identifiable information or other data subject to protection. CGI Third Parties shall commit to protecting CGI and client data by implementing appropriate technical and organizational security measures and ensuring timely notification to CGI of confirmed or suspected incidents involving CGI or client data. CGI Third Parties shall also cooperate with requests for validation of security practices. As required by applicable law and any agreements executed with CGI, all CGI Third Parties shall respect, and be responsible for protecting, the intellectual property rights of CGI and its clients, including, but not limited to, maintaining it in confidence and in secure work areas. CGI Third Parties shall seek ensure that their employees take CGI required training when provided and reasonably requested by CGI.

4.33 Physical and Environmental Security

The SIROMS SaaS in built upon the AWS FedCloud, which is mandated by its FedRAMP compliance to maintain all of these controls. Any further security concerns are outside of the scope of the SIROMS SaaS.

4.34 Contingency Planning

A detailed explanation of all backup and recovery strategies, including Disaster Recovery and Business Continuity are located in the Disaster Recovery and Contingency Plan located in Appendix C.

4.35 Incident Response

CGI implements a global security incident management process to handle all phases of a security incident. Responsibilities are clearly defined at all levels. Priorities are established to help ensure the timely resolution of incidents. Records of incidents are maintained and reported to senior management. High priority incidents are managed through CGI's Incident Management Centre (IMC), who coordinate with and escalate to all required parties based on priority. Collection and preservation of evidence are observed throughout the process.

Responsibilities are clearly defined at all levels. Priorities are established to help ensure the timely resolution of incidents. Records of incidents are maintained and reported to senior management. High priority incidents are managed through CGI's Incident Management Centre (IMC), who coordinate with and escalate to all required parties based on priority. Collection and preservation of evidence are observed throughout the process.

CGI incident management teams provide security incident notification and status updates to clients, authorities and/or individuals as required by local legislation generally applicable to IT service providers and/or as agreed in the client contract. Incident simulation exercises are periodically performed to help ensure the process works as expected when needed.

CGI will notify DCA-DRM if there is a breach in the contractually specified time frame.

- The organization has purchased a cybersecurity liability policy. CGI considers these documents as proprietary and confidential. As such we can 1) host a Teams meeting to walk the client through our policies and procedures, 2) Send them a copy of our Security Baseline Overview which provides a detailed overview of CGI's Security Program and Policies or 3) Make printed copies and bring them to the client's site to review in person. Option 3 is at the client's expense.

4.36 Tax Return Data Security

CGI along with DCA-DRM will utilize enterprise security management services that encompass the governance, strategies, frameworks, plans and assessments necessary to create and manage an effective enterprise-wide security program. CGI's focus is to work with our customers to articulate the appropriate governance and policies to achieve enterprise goals. This systematic approach establishes an overall risk management framework that takes into account the unique risk profile of SIROMS and the associated regulatory and privacy requirements. Security management goes beyond the physical levels that provide the access and control mechanisms for the facilities or infrastructure. It applies to protection of the software, applications, and data from corruption, or unauthorized intrusions to maintain integrity. Dealing with these possibilities involves the analysis of potential threats and requirements surrounding the level of protection needed by the State to help ensure data confidentiality and integrity as well as service availability.

CGI will work closely with the State of New Jersey to properly secure the PII stored in SIROMS. Within the Security Plan found in Appendix D, all systems are categorized based on which do or do not contain PII and all databases containing PII use transparent data encryption to help ensure that data at rest is encrypted.

5 Pricing Summary

A breakdown of the CGI pricing summary is provided in the subsequent sections.

5.1 Labor Pricing

As requested in the RFP, CGI has aligned the State Supplied Price Sheet labor categories with GSA labor categories. CGI has used the pricing from CGI's GSA rates based on the mapped GSA labor category.

State Supplied Rebid Labor Category	GSA Labor Category
Project Manager	Project Manager - 5
Senior Consultant	Functional Business Process Analyst -3
Junior Consultant	Functional Business Process Analyst -2

Since 2013, CGI has highly valued the partnership with New Jersey Department of Community Affairs. The SIROMS project has been highly successful to date because of the several highly skilled key personnel that CGI provides to DCA-DRM. Managing a project of this compact size and complexity requires a team of highly multi skilled functional and technical project managers across the three key pillars of the SIROMS hierarchy including, Functional & Quality Control, Application Delivery, and Database & Business Intelligence.

CGI has completed the exercise to best align our CGI partners to the labor categories provided by the state however, we feel it understates the actual role and responsibilities of several team leads. The following chart depicts how key personnel maps to the roles identified in the RFQ and our proposal to better align CGI Partners to their actual role and responsibilities on SIROMS. In addition, we are pleased to offer a discount to the supplied GSA rates identified in the column titled "***GSA Rate Aligned to State Supplied Role"*** which is discounted relative to the state supplied" GSA ***Rate".***

Key Personnel	GSA Role Mapping	GSA Rate	GSA Role Mapped to State Supplied Price Sheet	GSA Rate Aligned to State Supplied Role	State Supplied Price sheet Labor Category
Chandana Jampana	Software Developer/Programmer- 5	$223.89	Functional Business Process Analyst -3	$171.57	Senior Consultant
Diana Goldin	Functional Business Process Analyst - 5	$248.13	Project Manager -5	$197.87	Project Manager
Jim Rudd	Security Architect/Engineer -5	$286.15	Functional Business Process Analyst -3	$171.57	Senior Consultant
John Otchy	Functional Business Process Analyst - 4	$210.71	Functional Business Process Analyst -3	$171.57	Senior Consultant
Madhu Chandran	Data Architect – 5	$252.28	Project Manager -5	$197.87	Project Manager
Steven Ramroop	Helpdesk Specialist - 4	$132.99	Functional Business Process Analyst -2	$123.21	Junior Consultant
Tom Rispoli	Software Designer – 5	$237.77	Project Manager -5	$197.87	Project Manager
Vaid Ram	Program Manager -5	$282.22	Project Manager -5	$197.87	Project Manager
Vijaya Kasina	Software Developer/Programmer- 5	$223.89	Functional Business Process Analyst -3	$171.57	Senior Consultant
Zhitong Zhao	Software Designer - 5	$237.77	Functional Business Process Analyst -3	$171.57	Senior Consultant

5.1.1 Minimum Staffing Requirements

In order by meet the requirements specified in the RFQ, there are several skills sets that will need to be accounted on the SIROMS team. The following list contains minimum skills required to maintain the project:

- Project Management
- Server Administration
- Security Specialist
- Help Desk
- SQL Server
- SSRS
- SSIS
- Tableau
- Application development in the following areas
    - Metastorm BPM
    - Camel
    - C#/.net

5.2 Software/Services License Pricing

The following table lists all the software licenses that are part of the pricing.

Software/Services	License Terms	Comments
MBPM / ECM	User Based	CGI procures this license for DCA-DRM annually.
Tableau	User Based	CGI procures new licenses each year based on identified need.
SurgeMail	Perpetual License Annual Fee for Support	SurgeMail product requires annual maintenance fee for continued maintenance support.
FTP Server	2 Perpetual Licenses Annual Fee for Support	Cerberus product requires annual fee for continued maintenance and support includes updates/upgrades.
SSL Certificate (*.siroms.com)	Every two years	Issued every two years.
Domain (siroms.com/net/org)	Every two years	Registration of Domain required every two years.
SSL Certificate (IdaRecovery.us)	Every two years	Issued every two years.
Domain (IdaRecovery.us)	Every two years	Registration of Domain required every two years.
SSL Certificate (NJDRM.us)	Every two years	Issued every two years.
Domain (NJDRM.us)	Every two years	Registration of Domain required every two years.
ArcGIS - Maintenance	User Based	CGI procures this license for DCA-DRM annually.
Third Party Penetration Testing	Annually if requested by DCA-DRM	CGI will work with an independent third-party vendor to perform penetration testing exercises.

5.2.1 Software/Services Pricing Assumptions:

- The pricing for hardware and software maintenance provided in the State Supplied Pricing sheet are estimates based on third party products and licenses including average year over year increases. Third party software cost increases are beyond the control of any vendor to mitigate. In these instances, CGI will notify DCA-DRM of the specific increase and provide an updated quote for approval. An approval from the SCM is required prior to proceeding with the procurement.
- Any additional software not described in chart above is out of scope and will result in additional software increases.
- CGI understands that as good stewards of the grants provided to the State, we propose the following structure for Tableau licensing to reduce overall costs.
    - For the base years, a reduction in the total user licenses will begin in year two. A staggered year over year reduction of 5 viewer licenses per year for a total reduction of 15 by the end of year four. In addition, a one-time reduction of 2 creator licenses in year two per year carried over to years three and four for a total reduction of 2 creator licenses by the end of year four.
    - For the option years, the year five the breakdown of licenses starts with total of 20 viewers, 2 creators and 2 explorers licenses. Between year five and year ten, a reduction of 2 viewer licenses year over year. Year ten assumes 8 total viewers and 2 creators.

  - If the state is not amenable to the proposed licensing structure described above, it may result in additional costs to the state.

5.3 Hosting Pricing

During the first four years of the base contract award, it is anticipated that the project will be operating at peak capacity with key DCA-DRM programs and initiatives as priority requiring new development and modifications to SIROMS. SIROMS Hosting configuration for base years assumes the need for an appropriately sized DEV/UAT environments for the purpose of supporting development, testing, and deployment activities. For example, the UAT environment will be updated with regular data refreshes for the purpose of performing UAT testing and demos prior to delivering new code to production. The production environment assumes the infrastructure availability needs of the current environment continue through the end of the base year timeframe.

Beginning with option year five it is anticipated that the needs of the program will shift from software development to maintenance. In keeping with the client's needs to keep overall costs down, CGI would greatly leverage the AWS flexibility to provide reduced pricing for the option years.

Starting in option year five, no system or reporting development capacity is anticipated. Leveraging a feature in AWS to turn down servers, the entirety of the UAT environment will be turned off to reduce AWS Consumption costs. Specifically, the servers will only be turned on 6 hours a month for the purposes of server maintenance, including applying patches and upgrades to software stack. These servers will only be leveraged for the critical issues with the production environment. Any additional uptime requirements for UAT environment, including bug fixes will result in increases to the AWS cost.

This price quote assumes decreased user community in year four thus allowing for opportunities for server consolidation in the option years. Starting in year five, production LDAP File Server and Web servers may be consolidated with a decreased SIROMS user community activity. CGI will evaluate the performance of the individual servers and config the consolidated servers to meet the needs of the SIROMS user community.

5.3.1 Hosting Pricing Assumptions

- Software manufacturers may dictate minimum software or hardware requirements that may impact the sizing of individual servers hosting the software.
- DCA-DRM has described key performance requirements of the SIROMS application, CGI will work with the state to assess any additional hardware sizing requirements and adjust to meet key metrics DCA-DRM identifies as a priority.
- The sizing of the hardware may also be adjusted during instances when the software stack components require upgrades. For instance, the BPM/ECM upgrade will require an additional server transitional server for production testing prior to implementation. Servers procured for upgrades is recommended to be in place until two weeks after go live. CGI will work with DCA-DRM to schedule these activities and obtain approval for the updated pricing before proceeding with these activities.
- Another example is easing the Recovery Time Objective (RTO) as specified in the RFQ section 4.5.1. The infrastructure pricing discussed above includes hardware specifications to meet the documented RTO. Any opportunity to ease the RTO timeframe will provide immediate cost savings to the state.
- There may be savings gained from reserving hosting infrastructure through AWS. Whenever possible, CGI will look to reserve infrastructure and pass on savings to the state.

- External costs, beyond the control of CGI or the state, associated with third party vendors such as AWS and third-party software vendors may not remain constant across the length of the contract. For example, SIROMS Hosting Cloud Consumption costs are currently passed through from Amazon Web Services (AWS). If the rates from AWS Cloud Services increase, which are to be expected year over year, CGI will pass on these increases to the state.
- As we have seen in prior years maintaining SIROMS, space usage is not always consistent and periodic needs to increase storage space to accommodate increased document storage requirements will be necessary.
- Furthermore, the SIROMS application suite must also maintain stated performance goals. If performance goals are not being met due to increased demand or volume of data, it may become necessary to increase the processing power of the virtual infrastructure to ensure the application meets its performance goals at the expected user load. This would have the effect of increasing the infrastructure price.
- At cost to the DCA-DRM, CGI will employ qualified third parties to perform specific exercises like penetration testing and red team at the request of the state.

6 Appendix A – Resumes

Please see appendix A for detailed resumes for all management, supervisory, and key personnel to be assigned to the Contract.

7 Appendix B – Performance Management Plan

Please see appendix B for the draft Performance Management Plan.

8 Appendix C – Disaster Recovery and Contingency Plan

Please see appendix C for the draft Contingency Plan.

9 Appendix D – Security Plan

Please see Appendix D for the draft Security Plan.

10 Appendix E –Infrastructure Overview

Please see appendix E for the SIROMS Infrastructure Overview.

11 Appendix F Forms, Registrations and Certifications

The following forms, registrations and certifications are addressed in Appendix F.

1. Offer and Acceptance Page
2. Ownership Disclosure Form
3. Disclosure of Investment Activities in Iran Form
4. Disclosure of Investigations and Other Actions Involving Bidder Form
5. MacBride Principles Form
6. Service Performance Within the United States
7. Confidentiality/Commitment to Defend
8. Pay to Play Prohibitions
9. Affirmative Action
10. Business Registration
11. Certification of Non-Involvement in Prohibited Activities in Russia or Belarus Pursuant to P.L2022,C3

Subcontractor Utilization Plan is not applicable.

State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire submitted as a separate document.

12 Appendix G - Financial Capability of the Bidder

CGI has been a publicly traded company since December 17, 1986. CGI company shares are traded on the Toronto Stock Exchange (Symbol: GIB.A) and New York Stock Exchange (Symbol: GIB). CGI's Fiscal 2022 and 2023 Results are available for review at: https://www.cgi.com/en/investors/annual-reports. The following documentation regarding the Financial Capabilities of the Firm can be found at the link provided above.

- Balance Sheet
- Income Statement
- Statement of Cash Flow
- Notes from the most recent fiscal year

Printed copies of our latest annual report may also be requested at: https://www.cgi.com/en/contact-us.

CGI meets the meet the required insurance requirements and can provide proof upon contract award if requested:

- Professional Liability Insurance of not less than $1,000,000
- Cyber Breach Insurance of not less than $5,000,000