



October 1, 2021

NEW JERSEY STATE GOVERNMENT CRITICAL INFORMATION TECHNOLOGY NEEDS & FUNDING ELIGIBILITY

Submitted by:

CHRISTOPHER REIN
NJ Chief Technology Officer

CONTENTS

1.0 Purpose	1
2.0 Executive Summary	1
3.0 Critical IT Needs (Detail) and Specific Linkage to SFRF	2
3.1 Modernization of Outdated Computer Systems	2
Table 3.1 Legacy/Old Systems within NJ Executive Branch	3
3.2 Identity Management Across Executive Branch	4
3.3 Enterprise Data Center Upgrades.....	4
4.0 Additional Background Information	5
Table 4.1 FY20 IT expenditure areas for State of NJ Executive Branch.....	6
5.0 Additional Context and Strategic Focus for NJOIT in last 3 years	7
5.1 Cybersecurity Improvements	7
5.1.1 PAM (Privileged Access Management)	7
5.1.2 Enterprise Endpoint Protection	8
5.1.3 Multi-Factor Authentication (MFA).....	8
5.1.4 Network Resilience	8
5.2 Data Center Consolidation & Virtualization.....	9
5.3 Cloud Computing.....	9
5.4 Mainframe as a Service (MFaaS) Project	10
6.0 CIO and IT Leadership Responses – 3Q’ 2021 Critical IT Needs Survey	11
6.1 Question: “Please identify the <u>top 2 areas</u> you see as most in need of substantial investment in your agency” .	11
6.2 Question: “What do you see as the greatest barrier to meeting your Agency’s critical needs?”	11
6.3 Question: “Risk to Operations: what do you see as the greatest risk to your most critical IT systems?”	11
7.0 Conclusions and Recommendations	12

1.0 PURPOSE

This Report is submitted by the Chief Technology Officer to the Treasurer and the Joint Budget Oversight Committee in furtherance of language included on p. B-208 of the Appropriations Act.

[Notwithstanding the provisions of any law or regulation to the contrary, from the amount herein above appropriated for the Office of Information Technology, the Chief Technology Officer shall prepare a detailed report of the State government's most critical information technology needs. The report shall identify priority information technology projects that shall be considered for funding from federal funds provided or made available to the State from the federal "Coronavirus State Fiscal Recovery Fund" established pursuant to the federal "American Rescue Plan Act of 2021," Pub.L.117-2.]

2.0 EXECUTIVE SUMMARY

Within the Executive Branch, the current highest priority critical IT needs are:

- The modernization of several specific legacy systems
- The need for a Statewide Identity Management system
- Physical upgrades to the State's enterprise data center

These three areas of critical need are based on the degree of resident impact, the age and risk tolerance of the systems and infrastructure, and the magnitude of the modernization efforts that are needed. Of particular note are the older systems in use by the Department of Labor, the Department of the Treasury, parts of the Motor Vehicle Commission's infrastructure, Human Services, and the Department of Corrections' inmate systems. All these legacy systems are supporting critical State functions, and the failure of any one of them would have immediate detrimental impacts on resident facing services. Worse, the ability to quickly recover from a failure is in doubt as the aging infrastructure is more difficult to support and institutional expertise on the legacy systems is dwindling.

Modern IT systems have their foundation in identity. Without a strong identity system, it is impossible to provision specific users with access to services with additional roles to grant privileged access when needed. A legacy patchwork of varied identity solutions throughout the Executive Branch have led to silos of users, distributed infrastructure, and identity inconsistency. This impacts residents who may need varying number of accounts

to access different public facing State systems. It also impacts internal State operations as it becomes challenging to provision access to enterprise applications in a uniform, secure way.

Also among this top tier of the State's critical IT needs is the need to continue and accelerate making necessary upgrades to the State's data centers in West Trenton, NJ. The enterprise data center supports nearly all the executive branch's IT infrastructure, and it has not been substantively updated since its initial construction. In the event of a failure of the existing power and cooling systems, residents and state operations would be impacted with timelines to recover likely stretching into weeks.

3.0 CRITICAL IT NEEDS (DETAIL) AND SPECIFIC LINKAGE TO SFRF

In consultation with the Governor's Disaster Recovery Office (GDRO) to best determine the degree of eligibility for the critical IT needs listed herein, the following table provides a succinct assessment of eligibility. Improvements to data or technology infrastructure are generally eligible for SFRF funding in the categories of 1) Public Health and Health Programs and 2) Economic Relief Programs. A degree of complexity is introduced by the fact that most of these identified needs are multi-year efforts, and most require competitive bidding due to existing procurement requirements.

3.1 Modernization of Outdated Computer Systems

A number of NJ's large business applications were created many years ago. Some were developed by State IT staff, others were purchased from the market, still others were custom developed specifically by a vendor for the stated requirements of one of the State's agencies. These systems have been kept operational and functioning by agency IT staff and NJOIT personnel. In some cases, the operating platform for the application is antiquated, and the technology may have gone into an "unsupported" status. Within the table below, the order is not prioritized; rather, all are top tier IT critical needs.

Table 3.1 Legacy/Old Systems within NJ Executive Branch

Area of Critical Need	SFRF Eligible?	Notes & Duration Estimate
Full Modernization for Dept of Labor's Unemployment and Temporary Disability Applications	Likely	Likely to require 2-4 years as both the systems and business processes will change. Initial modernization funding for year-1 is allocated in State FY22 budget. Investment in the modernization or replacement of Labor's computer systems must be accompanied by business process and customer service operational changes; These changes and regulations set by Federal Unemployment requirements will require both State and Federal changes.
Department of Treasury's three highest risk and critical systems (Budgeting System, Tax Administration System, Accounting and Finance System)	Potentially	Some modernization planning efforts are slated to begin this Fiscal year, including that for the budgeting system. We may be able to meet eligibility requirements for the Tax Administration system under economic relief but would need to do a more thorough analysis.
Motor Vehicle Commission's Core Database and Application	Potentially	The computer systems that operate the State's Motor Vehicle Commission are an integrated set of modules and operating platforms; Some of these have been upgraded and modernized over the past 5 years; However, there are substantial components which rely on very old programming languages and legacy databases. These add operational risk, and often are a barrier to meeting the new and evolving needs to serve the NJ motoring public.
Department of Corrections OBCIS (Offender Based Correctional Information System)	No	This system has been unsupported for several years, meaning the vendor who provided the system is no longer in business. OBCIS is also used by Parole Board and the Juvenile Justice Commission.
State Payroll System	No	This may be the oldest single system within the Executive Branch. It is mainframe hosted and has limited ability to allow for making changes or application support for any new payroll strategies. This system is relatively stable.
Department of Human Services FAMIS (Family Management Information System)	No	FAMIS is an older system which operates on a platform that does not have robust support capabilities; therefore, DHS bears elevated risk in operating this platform Funding for the support and potential modernization of the system is from federal sources. Additional analysis is required to determine SFRF eligibility.
State Pensions System	No	A series of very old, mainframe-hosted systems to manage, track, and pay recipients of variety of different State pension groups.

3.2 Identity Management Across Executive Branch

Identity management makes sure that the right users have access to the right technological tools. Over the years, various State Agencies have implemented a variety of identity, authentication, and authorization products and schemes. These various and heterogeneous systems differ in their age, scope (internal vs. public facing), and vendor platform. Across the US, it has been shown, both in private sector large corporations and in State governments in the public sector, that “everything begins with Identity.” A building’s construction requires a solid base and foundation. Similarly, a strong identity management system and Statewide policy are needed to support all new, modernized, rebuilt, and upgraded IT systems that can offer NJ’s residents and State staff the secure, current technology that they need and deserve. Assessment by the Governor’s Disaster Recovery Office and NJOIT indicate that this IT infrastructure could qualify for Coronavirus SFRF funding. The criticality of a strong and effective identity management system across the Executive branch is a barrier to economic growth as it will slow down, and add risk to, the enablement of necessary and new resident services being delivered online. Permits, licenses, professional certifications, paying feed, etc. are all critical functions the State needs to improve and accelerate.

3.3 Enterprise Data Center Upgrades

The State’s Office of Information Technology and Treasury’s Division of Property Management have begun Phase One of a multi-year, five phase Enterprise Data Center refurbishment and upgrade that was years overdue. The electrical feeds, transfer switching, generator and battery backup systems will be receiving necessary upgrades to provide the stable and reliable power needed to support the Executive Branch. The Engineering firm contracted for the detailed assessment of the Enterprise Data Center and the first Phase of the construction have provided the estimate of \$64.3M over 5 fiscal years (through 2026). Year 1 was funded by an appropriation from the Capital Budget, and it is anticipated that future phases would similarly be funded by Capital Budget requests. In the event Capital Budget requests are not approved to support the upgrades to the Enterprise Data Center, the risks of a complete data center outage will remain and grow as the existing equipment ages.

4.0 ADDITIONAL BACKGROUND INFORMATION

The New Jersey Office of Information Technology (NJOIT) is designated as the exclusive government provider of IT infrastructure services¹ for New Jersey’s Executive Branch. NJOIT was originally formed in 1984 as the Office of Telecommunications and Information Services (OTIS) under Governor Thomas H. Kean via Executive Order. In 2007, the Office of Information Technology Reorganization Act established NJOIT in a more consolidated form. The organization was structured as an “in-but-not-of” Treasury, and it was composed of over 600 civil servants specializing in application development and hosting, network engineering, database administration, security operations, and other technology disciplines. The transition to this consolidated model occurred over several years yet was never fully implemented as some agencies retained some of their technology staff and did not transfer them fully to NJOIT. The State’s IT operational model was again restructured, with the responsibility for “IT infrastructure services” now consolidated under NJOIT as directed by Executive Order EO225 (Christie) in 2017. This structure moved the responsibility for application support responsibility out into each of the State’s Agencies. A summary chronology of NJOIT follows:

- EO 84 (Kean) established OTIS in 1984
- EO 87 (Whitman) abolished OTIS and created OIT in 1998
- EO 42 (Corzine) rescinded EO 87, and restructured OIT
- P.L.2007 c.56 The Office of Information Technology Reorganization Act
- EO 225 (Christie) defined NJOIT scope as Infrastructure technology

New Jersey’s Executive Branch, therefore, currently operates on a hybrid-consolidated model. A series of structural changes has challenged the consistent and strategic operation of information technology services.

Although the various line items for IT expenditures in NJ’s budget are spread across NJOIT and several Executive Branch agencies (like most other States that operate with a hybrid-federated model), NJOIT’s research and analysis indicate the total spend on IT in NJ falls between \$610M and \$630M, which is in the 1.4% range of State revenues.

¹ “Infrastructure services” refers to providing servers, mainframe operations, network, storage, e-mail, and secure cloud processing as well as the State’s websites and the MyNJ Portal.

Table 4.1 FY20 IT expenditure areas for State of NJ Executive Branch

Category:	FY20 Expenses (\$M)	Notes:
NJOIT Salaries	\$55	From OIT CFO
NJOIT Non-Salary	\$78	From OIT CFO
Agency Infrastructure Procurement	\$14	OIT Processed, Agency Funded
Agency Non-Infrastructure Procurement (Apps, Vendors...)	\$270	OIT Procurement Tracking
Agency IT Salaries	\$140 - \$160	Using Averages and HR Records
Estimated small (DPA) purchases by Agencies Not reported to NJOIT	\$50	Recommended study to confirm accuracy of this estimate
	\$610 - \$630M	This represents approximately 1.45% of State revenues.

5.0 ADDITIONAL CONTEXT AND STRATEGIC FOCUS FOR NJOIT IN LAST 3 YEARS

Government means delivering services to our residents. Today, we employ technology to deliver an overwhelming majority of these services. The implementation of new services, new and innovative channels of access, and remote work models are occurring at a rate that often outpaces traditional IT projects and procurement. It is therefore clear that dependable, secure, and agile infrastructure is more critical than ever to help State Agencies deliver services to their constituents. Several key areas of focus for NJOIT in the past 2-3 years have yielded accomplishments that include the following:

- Cybersecurity Improvements
- Development of Strategic Plan
- Data Center Consolidation & Virtualization
- Establish Cloud Computing Infrastructure
- Mainframe Migration

5.1 Cybersecurity Improvements

With implementations in FY19 through FY21, a major focus of the CTO's office has been addressing significant gaps and challenges in New Jersey's cybersecurity posture. These key accomplishments are described below.

5.1.1 PAM (Privileged Access Management)

NJOIT is underway implementing a product across the enterprise computing environment which protects and allows for the secure management of privileged credentials (administrative accounts).

The product automatically discovers and onboards (encrypts) privileged credentials used by administrators. Centralized policy management allows administrators to set policies for password complexity, frequency of password rotation, and detailed access control rules.

Automated password rotation helps strengthen security while eliminating time-intensive, manual processes for the IT teams. Prior to this implementation, credentials were managed on an ad hoc basis with substantially less secure measures.

5.1.2 Enterprise Endpoint Protection

NJOIT and the NJ Office of Homeland Security have together implemented an enterprise-wide Endpoint Detection and Response (EDR) technology in close partnership with the State agencies. It is a platform built to stop breaches, malware, and ransomware via a set of cloud-delivered technologies that both detect, and more importantly prevent, thousands of types of attacks. This product is the highest rated one within the industry. Attackers are now going beyond just viruses and malware to breach organizations; they are increasingly relying on exploits, zero-day vulnerabilities, and other hard-to-detect methods such as credential theft and social engineering. This product allows our Executive Branch IT staff to respond to those challenges and provides cyber threat intelligence and a statewide visibility dashboard capability to our Cybersecurity Communications and Integration Cell (NJCCIC) within the Office of Homeland Security.

5.1.3 Multi-Factor Authentication (MFA)

As recently as two years ago, the adoption and use of multi-factor authentication across the executive Branch was quite low. The NJCCIC and the State's Chief Information Security Officer (CISO) have published a statewide information security manual that each employee must abide by to protect the State's information and data. NJOIT has enabled and increasingly incorporated MFA in the MyNJ State Portal, in our e-mail and office systems, and for remote access to certain agency applications. In many cases, these are older systems, and were not created during a time when heightened security awareness nor data privacy needs were built in. Thus, the enablement of security measures like MFA becomes more difficult to add in later.

5.1.4 Network Resilience

Network resilience is the redesigning and modernizing of large operating portions of our State's secure network, the Garden State Network (GSN). For the past three years this has been, and continues to be, a high priority for NJOIT. Partnering with Homeland Security's NJCCIC for resilience planning, testing, and implementation, this project reduces risk by improving the State's security posture. Fewer portions of our GSN are now visible or accessible from bad actors outside the GSN via the Internet. NJOIT is also presently investing in upgrading the network infrastructure with large high-capacity devices called "next generation" firewalls & routers. The upgrading of the State's network can never remain static; rather, the increases in demand, more sophisticated needs by our Agencies, and continually evolving threats all require constant vigilance, planning, and response.

5.2 Data Center Consolidation & Virtualization

The goals of NJOIT's IT Consolidation efforts include the centralization of IT infrastructure, data center operations, and the provision of all related underlying services that support the Executive Branch business applications. This consolidation is accomplished primarily through a series of shifts of accountability and ownership of computing assets. When referring to computing assets, this includes servers, storage units, routers, switches, mainframes, and other devices that power the Garden State Network and the 600+ software applications that operate the Executive Branch. Tactically, the most common methods of consolidation involve "virtualization technologies" and in some instances, the physical relocation of Agency-based physical infrastructure into the NJOIT Enterprise Data Centers. The areas of impact are people, process, technology, and service delivery. Equally important are placing major emphasis on infrastructure modernization, technology standardization, enhancing the infrastructure security posture, optimization of services delivery, the stabilization, and availability of services for the Executive Branch and the residents of the State of New Jersey.

5.3 Cloud Computing

Three years ago, the State of New Jersey had no cloud environment in which to allow our Agencies to securely build and operate applications. In recognition of the strategic value that public cloud services can provide to the State, NJOIT has invested substantially in the creation of an Executive Branch public cloud service. This effort focused on creating a method of operations, procurement processes, establishing connectivity, skills building, and foundational cloud security design. NJOIT now offers accessibility to two cloud environments, with ease of use and accessibility for state agency business needs. The groundwork and foundation laid in building a highly available and secure platform was instrumental in quickly responding to the pandemic and serving New Jersey's residents.

By March of 2020, because most of the foundation had already been laid in our two enterprise cloud environments, NJOIT was able to support the pandemic response rapidly. We were able to provide cloud access quickly for the Department of Health and the Motor Vehicle Commission without lengthy procurements, server-building, or lengthy provisioning. We now provide computing power and storage to our agencies in the cloud in a matter of hours, instead of weeks or months. This delivers better services to the residents of New Jersey. Never had the State encountered the demands and challenges presented by a global pandemic; but never has NJOIT been able to respond so quickly with essentially limitless, scalable infrastructure to meet these demands. And this capability is in part due to our investment in the use of the Cloud.

5.4 Mainframe as a Service (MFaaS) Project

Before modern servers and personal computers, the Executive Branch owned and operated a large mainframe platform that hosted the State's most critical applications (Labor, Treasury, Motor Vehicle, State Police, etc.). On a regular mainframe replacement/refresh cycle, the State NJOIT would purchase large mainframe processors and storage systems and our IT staff would support this infrastructure, operating systems, and platform resources. As the State was approaching a refresh cycle in 2021, expensive hardware combined with the public sector's inability to compete with the private sector to attract and retain staff with specialized mainframe skills drove NJOIT to explore ways to mitigate these challenges. More than 250 of the Executive Branch's most critical workloads were still supported by this mainframe platform. So, while some agencies had modernization efforts underway, NJOIT needed to implement a more sustainable long term support approach.

After more than a year of planning, budgeting, and contract work, NJOIT successfully migrated the Executive Branch's legacy mainframe platform into a Mainframe-as-a-Service (MFaaS) model. This is a vendor-hosted mainframe platform, and the migration was completed in June 2021. Under this model, the State no longer must purchase physical mainframe hardware. Rather, the State consumes virtualized mainframe resources – computing and storage – and pays only for the resources we consume. The vendor hosts, manages, and supports the hardware infrastructure and the operating systems while our State staff manage the licensing and support of third-party software products, CICS, databases, and applications. The vendor and the State are jointly responsible for satisfying applicable regulatory and compliance controls applicable to the regulated data on the platform.

6.0 CIO AND IT LEADERSHIP RESPONSES – 3Q’ 2021 CRITICAL IT NEEDS SURVEY

As part of the data gathering to prepare for this report, information was sought from 23 of the State’s Agency CIOs. This information was focused on the critical needs of, and the greatest barriers to, providing the business and technology solutions needed to advance IT. Of course, with the heterogeneous nature of these Executive Branch agencies, the responses differ, and this was fully expected. However, several clear trends and commonalities emerged. Below is a summary of the more standout issues.

6.1 Question: “Please identify the top 2 areas you see as most in need of substantial investment in your agency”

The top 3 responses (in order) within the results were:

- New business application(s) to satisfy new business or resident needs that are not met by existing legacy applications.
- Replacement/refresh/upgrade of existing infrastructure
- Refactoring (re-writing) existing applications in new language or new platform to allow current support

6.2 Question: “What do you see as the greatest barrier to meeting your Agency’s critical needs?”

The top 3 responses (in order) within the results were:

- Staffing/IT talent (recruit & retain)
- Procurement challenges stemming from contractual difficulty
- Funding/financing

6.3 Question: “Risk to Operations: what do you see as the greatest risk to your most critical IT systems?”

The top 2 responses which dominated the results were:

- Attracting IT staff due to compensation disparity and work environment in the market versus private industry
- Recent or impending loss of key staff with institutional knowledge

7.0 CONCLUSIONS AND RECOMMENDATIONS

This report identifies several areas of critical IT needs for the State of NJ Executive branch. An assessment of these critical needs indicates that a subset of these would be eligible for Coronavirus State Fiscal Recovery Funding.

One clear area of the State's critical needs is the replacement or modernization of several very old computer systems, each of which serve core functions of one of our State agencies.

Also among the greatest risk areas and largest challenges for IT operations across the Executive Branch is the recruiting and retention of highly skilled technology staff, and contractual procurement. Although this shortage of IT talent exists across both private and public sectors, the impact is more pronounced, and therefore the resultant risk is greater, to public sector enterprises, such as the State's Executive Branch Agencies.