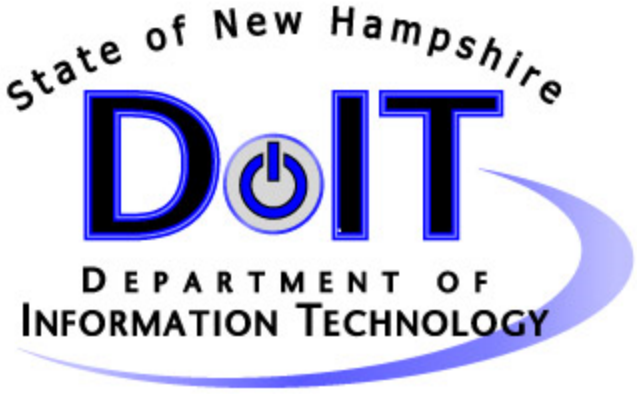

SFY 2022-2023

Capital Budget

Request Summary

Denis Goulet, Commissioner/CIO – June 2020

DoIT Capital Budget Requests

1. Cybersecurity Program Initiatives (Enterprise)-$2,086,000
2. Cloud Services (Enterprise)-$3,449,700
3. Continuity of Operation and Disaster Recovery (Enterprise)-$871,487

Total for DoIT's FY 2022/2023 Capital Budget Requests – $6,407,187

SFY 2022-2023 DoIT Capital Budget - Priority #1

Cybersecurity - Program Enhancement (Enterprise) - $2.086M

Main Objectives: Significantly improve the state's ability to protect the confidentiality and integrity of sensitive citizen and agency data from malicious cyber attackers and provide robust data breach prevention and detection in the state's expanded remote workforce and cloud-centric environment.

(1) Monitor and manage in real time the flow of sensitive personal, health-related or federally-protected citizen information both to and from state systems to systems and applications in cloud-based applications or to other external systems such as those hosted by federal agencies. This initiative will ensure that the state complies all federal compliance mandates (such as HIPAA) regarding the collection, transmission and storage of sensitive personal, health-related and other federally protected data.

(2) Implement a capability that provides positive identity verification across all systems, networks and applications for Executive Branch employees. This capability will provide positive protection against all phishing attacks; consistent identity for access to multiple systems and applications without multiple passwords; and eliminates the need for users to create and change passwords at regular intervals.

(3) Expand and enhance real-time cyber threat detection, analysis and blocking capabilities of our Intrusion Prevention System (IPS), allowing the state to detect and block malicious cyber activity before it can affect state systems and citizen data

Impact (if not approved)

The NH Cyber Integration Center (NHCIC) will not be able to apply the necessary cyber tools, threat intelligence and capabilities to adequately monitor and protect the flow of sensitive data within the state's networks and systems against the advanced persistent cyber threat.

SFY 2022-2023 DoIT Capital Budget - Priority #2

Cloud Services (Enterprise) - $3.450M

Main Objectives: DoIT requests a capital appropriation to obtain services and tools to design, develop, implement and provide cloud solutions that will enable and modernize digital government services and enhance existing infrastructure capabilities. The state's current environment does not fully utilize common cloud enterprise collaboration, case management and infrastructure solutions that have significant potential to improve the state's ability to serve its citizens and businesses. The total estimated $3.825M operating expenditures covers software subscriptions to be purchased by executive branch agencies through the operating budget.

This effort is intended to promote the following:

1) Provide transparent, flexible, and scalable platforms that can adapt to changing business needs

2) Allow the state to react quickly when disasters occur that require increased remote work capabilities and extended data access

3) Minimize the impact on the state's infrastructure as state agencies expand citizen services

Impact (if not approved)

Inability to provide constituent services in a timely and efficient manner, limits the state's ability to expand remote access usage for the state's workforce, and prevents the state from providing a more adaptive infrastructure environment during times of critical need.

SFY 2022-2023 DoIT Capital Budget - Priority #3

Continuity of Operation and Disaster Planning (Enterprise) - $871,487

Main Objectives: Provide the Information Technology services needed in order to implement cloud based infrastructure to accommodate continuity of operation (COOP) and disaster recovery (DR) services to DoIT based on business needs currently being gathered in the FY20/FY21 biennium funded with existing capital appropriation. In essence, this would improve the ability of NH agencies to support its citizens and businesses during emergency conditions that could potentially disrupt critical services.

This effort is intended to promote the following:

1) Protection against unexpected events affecting the delivery of DoIT services provided from the Primary Data Center by implementing the Disaster Recovery Plan created in FY21 using capital funds

2) Training of DoIT personnel to provide business continuity of operations in the occurrence of an unexpected event

3) Improved security against attacks on the Primary Data Center such as ransomware and cyber attacks

4) The prevention of data loss

5) Infrastructure required to provide disaster recovery services in the event the State's primary data center services are not available

Impact (if not approved)

Inability to provide critical services to the citizens of NH and state agencies. Potential of long recovery times in the occurrence of a disaster.