



57 ^{MLC}

STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
 27 Hazen Dr., Concord, NH 03301
 Fax: 603-271-1516 TDD Access: 1-800-735-2964
 www.nh.gov/doit

Denis Goulet
Commissioner

March 8, 2022

The Honorable Karen Umberger, Chairman
 Fiscal Committee of the General Court
 State House
 Concord, NH 03301

His Excellency, Governor Christopher T. Sununu
 And the Honorable Council
 State House
 Concord, NH 03301

REQUESTED ACTION

Pursuant to the provisions of RSA 14:30-a, VI, authorize the Department of Information Technology (DoIT) to accept and expend \$6,744,385 of American Rescue Plan (ARP) State and Local Fiscal Recovery Funds (SFRF) to implement a Cyber Insurance/Protection Program to replace and enhance current cyber insurance solutions, upon approval by the Fiscal Committee and Governor and Executive Council, through June 30, 2023. This is an allowable use of ARP FRF funds under Sections 602(c)(1)(A) or 602(c)(1)(C), for either provision of government services to the extent of the reduction in revenue or to response to the public health emergency or its negative economic impacts. **100% Federal Funds.**

Funds are to be budgeted in FY2022 and FY2023 with the authority to adjust between state fiscal years through the Budget Office if needed and justified. Funds are to be budgeted in FY2022 and FY2023 in the new accounting unit as follows.

01-03-003-030010-26xxxxx¹ Department of Information Technology, ARP Cyber Protection Program.

Class	Description	FY22 Requested Budget	FY23 Requested Budget	FY22/FY23 Total Requested Budget
038-500177	TECHNOLOGY SOFTWARE	\$5,395,915		\$5,395,915
040-500800	INDIRECT COSTS	\$2,500	\$2,500	\$5,000
041-500801	AUDIT FUND SET ASIDE	\$6,245	\$500	\$6,745
046-500465	CONSULTANTS	\$840,362	\$496,363	\$1,336,725
	TOTAL EXPENSES	\$6,245,022	\$499,363	\$6,744,385
Source of Funds				
000-16-400338	FEDERAL FUNDS	\$6,245,022	\$499,363	\$6,744,385
	TOTAL REVENUE	\$6,245,022	\$499,363	\$6,744,385

EXPLANATION

¹ All direct program costs will be accounted for using activity 00FRF602PH0304A and all administrative and indirect costs will be accounted for using activity 00FRF602PH0304Z. Accounting classifications may be subject to technical changes at the discretion of the Department of Administrative Services' Division of Accounting Services.

The Honorable Karen Umberger, Chairman
Fiscal Committee of the General Court

His Excellency, Governor Christopher T. Sununu
And the Honorable Council
March 8, 2022
Page 2 of 3

Since the early days of the COVID-19 pandemic the volume and severity of attempted cyber attacks on State of New Hampshire systems has increased dramatically and has not returned to pre-COVID levels. The response to this increased risk by cyber insurance carriers has been to scale back coverage and increase costs, to the point where traditional cyber insurance no longer adequately mitigates our risk.

The advent of Ransomware has changed the way states are now approaching cyber risk management. The traditional concept of insurance is that you have it there to cover you if something happens. In the case of ransomware, states cannot afford to let it happen because of its ability to effectively stop critical state services for extended periods of time. As a result states are effectively switching from a reactive risk management approach (cyber insurance) to a proactive one.

The Department of Information Technology respectfully requests ARPA funding in the amount of **\$6,744,385** to implement a proactive cybersecurity self-insurance and protection program through December 2026. The program will cover all branches and the Secretary of State's office and will contain the following components:

- **Incident Response (Cyber Forensics) Retainer** – Establish a contract with an appropriate entity to leverage at a moment's notice to provide the deep technical skills that we do not carry in house.
- **Cyber Negotiations Retainer** – Establish a contract with a cyber service that negotiates with Ransomware actors to reduce what the affected organization must pay to get their data back.
- **Managed Detection and Response (MDR) Services** - Currently, DoIT has a small team that monitors for cyber-attacks, but this is limited to the typical work day. As a result, most attacks are launched at night, on weekends or during holidays. Managed detection and response services provide 7x24x365 remotely delivered modern security operations center (MSOC) support, which allows organizations to rapidly detect, analyze, investigate and actively respond through threat mitigation and containment.
- **Endpoint Detection and Response (EDR) Solutions** - An "endpoint" is any device (PC, tablet, mobile phone, server, et al) that is connected to our state network. Currently there are ~22,000 endpoints on the state's networks. Successful ransomware attacks always start at a single endpoint and move on from there to impact as many endpoints as possible. For this reason, it is critically important that endpoints are equipped with instrumentation that will detect anomalies and that appropriately skilled personnel are available to respond immediately when the instrumentation reports unusual or inappropriate behavior. EDR service companies develop and maintain the necessary endpoint instrumentation to spot the anomalies when they occur. These companies recruit top tier professionals and benefit from economies of scale to provide these services 7x24x365 less expensively and more effectively than states can themselves, thus closing another weak spot in similar state provided services.
- **Cybersecurity Testing and Remediation** - As with several other important disciplines in the State of New Hampshire it is important that we perform independent 3rd party verification that our cybersecurity program is operating effectively and according to best practice. This item would fund biennial testing starting in 2022 which is appropriate as our most recent testing (funded by a prior capital appropriation) was completed in 2020. Testing will almost always identify areas for improvement so there is funding included for remediation.

Funds are to be budgeted as follows:

Class 038 - Technology, Software: Managed Detection and Response (MDR) and Endpoint Detection and Response (EDR) Licensing Bundle

Class 040 - Indirect Expenses: Budgeted at a rate of 10% of direct costs up to the first \$25K of any contract outsourcing functions or sub awards

The Honorable Karen Umberger, Chairman
Fiscal Committee of the General Court

His Excellency, Governor Christopher T. Sununu
And the Honorable Council
March 8, 2022
Page 3 of 3

Class 041 - Audit Fund Set Aside: to comply with RSA 124: 16 that requires all agencies that receive federal funds to set aside a percentage (0.1 %) of the federal revenue amount received to pay for financial and compliance audits.

Class 046 - Consultants

- Incident Response Cyber Forensics Retainer
- Cyber Negotiations Retainer
- Cyber Testing and Remediation

The following information is provided in accordance with the Comptroller's instructions memorandum dated September 21, 1981

1. **Personnel involved:** Temporary consultants.
2. **Nature, Need and Duration:** for the purpose of hiring independent professional services for cyber threat analysis support and assistance with the management of platform and resource utilization.
3. **Relationship to existing agency programs:** Builds upon DoIT's previous efforts in response to the COVID-19 public health emergency across all state agencies and partnerships relative to the COVID-19 response efforts.
4. **Has a similar program been requested of the legislature and denied?** No.
5. **Why wasn't funding included in the agency's budget request?** It was not known at the time that DoIT would be applying for American Rescue Plan (ARP) State and Local Fiscal Recovery Funds (SFRF).
6. **Can portions of the grant funds be utilized?** This request is 100% federally funded.
7. **Estimate the funds required to continue these positions:** \$0.00. The temporary consulting positions will not be continued beyond the time frame of the American Rescue Plan (ARP) State and Local Fiscal Recovery Funds (SFRF)

In the event that Federal Funds are no longer available, General Funds will not be requested to support this program.

Respectfully submitted,



Denis Goulet
Commissioner