I. Project Identification

FY2021

Project Title
Enterprise Cybersecurity Improvements

Agency: Department of Administrative Services

	Name	Phone	Email
Proposal Submitter	Jeff Brown	860-622-2218	jeff.brown@ct.gov
Chief Operating Officer	Josh Geballe	(860) 713-5100	josh.geballe@ct.gov
Agency IT Director	Mark Raymond	(860) 622-2419	mark.raymond@ct.gov
Agency CFO	Jolita Lazauskas	(860) 713-5145	jolita.Lazauskas@ct.gov
OPM Budget Analyst	Chris LeMay	(860) 418-6206	chris.lemay@ct.gov
Executive Sponsor	Josh Geballe	(860) 713-5100	josh.geballe@ct.gov
Agency LEAN Coordinator	Michael Barrera	(860) 713-5267	Michael.Barrera@ct.gov
Agency Data Officer	Michael Barrera	(860) 713-5267	Michael.Barrera@ct.gov

II. Project Details

A. Project Dates

Proposed Start Date	Expected Completion Date	Project Duration (months)
June 11, 2021	6/30/2023	24

B. Project Description - Provide a brief high level summary of the project in plain English without technical jargon that also includes the purpose and importance of the project. This information will be used for reporting the project to the Governor, General Assembly and Connecticut Open Data website.

This capital program is intended to reduce the likelihood of a large cybersecurity event within state government and to limit the impact of such an event should one occur. Cybersecurity threats are on the rise across the country, including major disruptions of government services in Atlanta, Baltimore, Texas, and Colorado. The State of Connecticut identified the need to improve our preparedness and defenses against these threats. The type and volume of the data that the state collects make us an attractive target for cyber criminals. The cost to recover from a breach also continues to grow.

This project bootstraps the cybersecurity program that supports all Executive branch agencies and the 30,000-plus state employees who use the enterprise network to support citizen services and agency functions daily. It includes equipment upgrades for external network boundaries and systems to monitor and respond to internal threats. Automation and integration with existing security systems will improve response times to security events by state IT staff. These improvements will make the state IT environment more secure and more responsive to threats and will reduce the burden on all Executive branch agency staffs to respond to cybersecurity threats.

C. Summary

Summary - Describe the high-level summary of what needs to be implemented to complete the project
This program of work lays the foundation for the cybersecurity program for the State of Connecticut including supporting the Statewide IT optimization efforts. This effort will increase the velocity of the current cybersecurity efforts and inject much-needed capital and consulting resources into the program.

D. Business Goals

Business Goals - List up to 5 key business goals you have for this project, when (FY) the goal is expected to be achieved, and how you will measure achievement, Must have at least one. Please use action phrases beginning with a verb to state each goal. Example: "Reduce the Permitting process by 50%". In the Expected Result column, please explain what data you will use to demonstrate the goal is being achieved and any current metrics.

Business Goal (Action Phase)	Target FY for Goal	Current Condition	Expected Result
Build and manage a full cyber vulnerability management program	FY 22	A modernized security vulnerability tool has been deployed, but no framework has been put around the management and remediation of known issues.	Create an agency-by-agency "score card" and address critical and high-risk vulnerabilities as a priority. Determine an ongoing management process and turn this into an ongoing operational activity.
Build and establish a full IT compliance program	FY 22-23	A single resource has been hired to help manage IT compliance issues including FTI audits, HIPAA, PCI and other requirements. No tools or other resources are available to support this function.	Deploy a Governance, Risk and Compliance (GRC) system to ensure accurate audit tracking and mitigation strategies for federal regulatory compliance systems. This will also provide a single source of information to track audit information from year to year. This will include a 3rd party risk management program.
Create an application security function that is capable of commercial, developed and cloud applications.	FY 22-23	Network architecture is not optimized for security response and modern design capabilities. Continued migration to the cloud requires security analysis and mitigation.	Establish a full architecture/engineering capacity that includes application security review capabilities.
Establish an incident response capability and improve forensic capabilities.	FY 22-23	Incident response is currently ad-hoc and highly dependent on key resources. There is no automation in place.	Establish tools, personnel and training to support responding to daily incidents and more proactive table-top exercises. Establish automation where feasible and practical.

E. **Technology Goals** - From a technical perspective, following the above example, list up to 3 key technology goals you have for this project and in which Fiscal Year (FY) the goal is expected to be achieved. Please use action phrases beginning with a verb to state each goal. Example: “Improve transaction response time by 10%".

Technology Goal	Target FY for Goal	Current Condition	Expected Result
Replace end-of-life Intrusion Prevention Systems with equipment able to inspect encrypted network traffic. Deploy these systems in a modernized network architecture that improves risk management and improves performance for agencies	FY 22	Current Intrusion Prevention Systems will not be supported in FY21 and are not capable of inspecting all network traffic. Network architecture does not yet take full advantage of segmentation.	Network boundary redesign complete with updated security systems and improved performance in network service to all Exec agencies.
Implement an automated Incident Response Management system to reduce response time to internal cybersecurity events such as malware or unauthorized use	FY 22/23	Incident response requires staff integration of inputs from multiple security and management systems to detect, analyze, remediate, report and track. This affects all state agencies.	Deploy an integrated response system that automates actions to reduce response time, particularly detection and remediation. Tracking system that is shared across all state agencies
Increase licensing (EPS) for the Security Incident and Event Management system to log critical enterprise devices/servers to ensure reduced response time for malicious cybersecurity events.	FY 22	The current system receives all FTI environment device logs, along with a few other critical network logs. Expansion is required to ensure all critical network equipment can log to the system for event and incident monitoring and aid in the	Modernize security event monitoring and establish the capacity to review both Exec branch and agency events.

F. **Priority Alignment -** The criteria in this table, in concert with other factors, will be used to determine project priorities in the capital funding approval process. Briefly describe how the proposed projects will align with each criterion.

Priority Criterion	Y/N	Explanation
Is this project aligned with business and IT goals of your agency?	Yes	This project improves the ability of all state agencies to maintain the integrity and security of the enterprise network. Agency applications and citizen data residing on the network will be more secure and less vulnerable to interruption of service.
Does this project reduce or prevent future increases to the agency's operating budget?	Yes	This project updates systems and provides functionality that multiple state agencies require to meet compliance with federal guidelines. Deployment as an integrated enterprise service will reduce the requirement for individual agency costs in the future.
Will this project result in shared capabilities?	Yes	The security monitoring and response systems incorporated in this project will allow multiple agencies to leverage new capabilities to prevent and respond to security incidents and vulnerable conditions. Enhanced scanning capabilities will be available to all agencies to reduce risk.
Has the agency performed due diligence to determine if a solution that is currently being used by other state agencies or other states can be leveraged?	Yes	These systems are dedicated platforms for the physical network environment and the capabilities provided exceed other state agencies.
Is this project being Co-developed through participation of multiple agencies?	Yes	Agency input will be integral to this process and they will be consulted with on an ongoing basis.

G. **Organizational Preparedness** - The criteria in this table will be used to determine project implementation capabilities, governance and commitment.

Preparedness Criterion	Explanation
How will your agency be compliant with the *Management of State Information Technology Projects policy?* Provide any compliance details to date.	The cornerstone of the cybersecurity program will be a comprehensive policies and standards framework. We will be in compliance with all existing polices. Please note that dedicated project managers will be used from both internal and external sources
Explain the key milestones or activities that need to be completed as part of the project.	Concurrent milestones for internal security improvements would be installation of the Incident Response system, creation of the IT Compliance function, implementation of a Privileged User Management system, and deployment of the enhanced vulnerability scanning capability.
Describe the level of commitment that senior management will provide to the project.	This effort will be reported to all levels of management including the Statewide IT calls, ITSOR and Cybersecurity Committee meeting. It is anticipated that high-level milestones will be discussed at the agency commissioner's meeting.
Will, or has, the agency gone through a LEAN process improvement initiative related to this project? Provide a summary of the LEAN activities.	This is an infrastructure improvement focused project that is not matched with a LEAN initiative; however we have a LEAN expert on staff and will take advantage of her knowledge and best practices.
How is the agency prepared for and experienced in Vendor Management?	The agency is experienced with multiple vendors in this technical area. Many likely vendors have already been identified.
Please indicate if the agency has provided up to date information on the Information Technology Project Portfolio and the Information Technology Application Portfolio SharePoint sites?	~~N/A~~ Yes, this has been provided.
Describe what procurement vehicles are expected for this project such as RFP, use of existing state contract, ITB, etc.	Existing state contracts will be used to procure the equipment and required support services to complete this project
How is the agency prepared to support this system once implemented (post-production support)? Who will host the solution?	Agency IT staff will operate and maintain these systems after implementation. The solutions will be hosted in the state Data Centers in Groton and Springfield or else will be cloud-based solutions that are vendor-supported.

H. **Project Ramp Up** - If capital funds are awarded for this project, how long will it take to ramp up? What are the key ramp-up requirements and have any of these already been started? For example, has a project manager been identified? Has an RFI been issued? Is a major procurement required such as an RFP?

This project will be able to ramp up immediately once funds are awarded. Internal design discussions and research have been in progress for the past 12 months regarding elements of this comprehensive project. Product research for component technologies has been conducted. Identification of a dedicated project manager and phased implementation of the network redesign and installation of updated systems will follow in FY21 and continue through FY23. It is not anticipated that an RFP will be required.

I. **Post Production Support** - Do you have the experienced staff with the proper training to sustain this initiative once it's a production system? Do you anticipate having to hire additional staff to sustain this? What training efforts are expected to be needed to maintain this system?

Current experienced staff will require training to operate and support updated systems once they are in production. Additional staff is not anticipated to sustain these systems once in production. Training efforts consistent with current levels will be needed to maintain these systems.

J. **<u>Financial Estimates</u> -** From IT Capital Investment Fund Financial Spreadsheet

Estimated Total Development Cost	**Estimated total Capital Funding Request**	**Estimated Annual Operating Cost**	**One Time Financial Benefit**	**Recurring Annual Financial Benefit**
	$ 11,000,000	$ 400,000	$ 0	$ 0

Explanation of Estimates

Capital funding includes hardware, software, professional services, training and project management to design, deploy and operate improved security architecture at the network boundary and internal systems to detect, respond to, and track cybersecurity events, as well as improve secure management of the state network environment. This will include expenditures over FY22 through FY23 to complete all milestones.

Assumptions: Please list key assumptions you are using to estimate project development and implementation costs

While new people resources are being added to the cybersecurity group, during the “build phase” we may not have the necessary expertise in house and will require some third-party consulting resources, as outlined in the proposal.

III. Expanded Business Case

A. Statutory/Regulatory Mandates - 1) Cite and describe federal and state mandates that this project in intended to address. 2) What would be the impact of non-compliance?

Statutory / Regulatory Mandates:
This project supports compliance with HIPAA, IRS Publication 1075 for the handling of Federal Tax Information, Criminal Justice Information System (CJIS), Payment Card Industry (PCI) standards, Privacy Act, and the Centers for Medicare & Medicaid Services (CMS).

Impact of non-compliance:
Non-compliance can result in suspension of state agencies or application from the use of CMS, IRS, FBI or payment card information or systems. It can also result in fines and other reputation damage.

B. Primary Beneficiaries - Who will benefit from this project (citizens, businesses, municipalities, other state agencies, staff in your agency, other stakeholders) and in what way? Please be specific.

The primary beneficiaries of improved cybersecurity for the state enterprise network environment are Connecticut citizens and state agencies. Citizen's information held in the state network will be better protected from cybersecurity incidents or criminal activity. State agencies will experience better security for their systems to conduct daily business. All state agencies will experience more rapid response to system compromises with automation that will allow for quicker identification and isolation of affected systems, and fewer systems affected overall, reducing staff effort required to maintain working systems.

Important:

- **If you have any questions or need assistance completing the form please contact Jim Hadfield or John Vittner**

- Once you have completed the form and the IT Capital Investment Fund Financial Spreadsheet please e-mail them to John Vittner and Jim Hadfield.

John Vittner, (860) 418-6432; John.Vittner@ct.gov Jim
Hadfield, (860) 418-6438; Jim.Hadfield@ct.gov