Corporate Security
2025-2029

1. Project / Program Summary

Type: ☐ Project ☒ Program	**Category: ☒ Capital ☐ O&M ☐ Regulatory Asset**
Work Plan Category: ☐ Regulatory Mandated ☒ Operationally Required ☐ Strategic	
Project/Program Title: Corporate Security – Company Wide Camera Rollout Program	
Project/Program Manager: Sean O'Connor	**Project/Program Number (Level 1):** 20283654
Status: ☐ Initiation/Planning ☐ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date: January 2014 (ongoing program)	**Estimated Date in Service: Ongoing program**
2025-2029 Funding Request ($000) **Capital: $6,168** **O&M:**	

Work Description:

The company uses 2,400 cameras throughout the system that are linked to our 24/7 Security Operations Center. Many of the fixed and pan/tilt/zoom ("PTZ") cameras have exceeded their expected lifespan (five to seven years) and need to be replaced. Also, the recent advances in camera technology, especially video analytics, enable the ability to tailor and adjust the video recording to specific threats and concerns. The Company began this program in 2014 as part of a yearly replacement program and expanded the program to provide camera coverage at company locations beyond just the most critical sites. The Company classified the project as Common Utility Plant in Service – General Plant – Miscellaneous Equipment.

In 2022 we replaced 83 legacy cameras with internet protocol ("IP") cameras, along with all related equipment.

In 2023 we replaced 104 old cameras with internet protocol ("IP") cameras, along with all related equipment.

In 2024 we have replaced 142 old cameras with internet protocol ("IP"), along with all associated equipment and expect that number to grow by the end of the year.

Each site has different challenges such as: internet (network) cabling; layout of the property and assets to be protected; obstructions; vendor labor; internal labor costs; lighting and available power sources which directly affects the amount spent on each location.

In 2023, the amount allocated to this program was increased from $1 million, to $1.2 million every year, taking advantage of technological improvements in equipment such as edge video analytics being used to detect intruders as well as advances in the ability to capture images in low light conditions , and combining it with installing new cameras to provide more enhanced security protection of our facilities especially on access/egress points and perimeter coverage. This request will provide the funding for buying cameras, cabling, switches, and all other related equipment plus the related internal and

vendor labor for installation.

In 2019, a small testing facility was established to conduct live in field testing of new technological equipment such as cameras, card access equipment and intrusion detection systems. This facility has proven to be very useful.

for the testing and vetting of new equipment with relation to live field conditions as well as compatibility with the IT network. Moving forward the goal is to enlarge this testing area to a bigger footprint to include installing additional areas with our standard anti-cut/climb fencing to bring the testing/vetting of new cameras and related equipment to the next level. Efforts would include acquiring and installing the latest technologically advanced cameras at the testing location to simulate true live conditions. This testing process would also give a qualitative and quantitative view of what technological equipment best suits the environment.

Justification Summary:

As the Company enhances its electronic security measures, the number of cameras being installed and connected back to our Security Operations Center continues to increase. These new camera installations are all IP based and the existing stock of outdated analog cameras/CCTV equipment needs to be replaced to match the newer technology. Eventually the original IP cameras installed will also reach the end of life (5-7 years) and will need to be updated as well.

Cameras have a dual purpose of protecting our assets from theft, vandalism and sabotage and providing a safety measure for our employees. The replacement of the outdated CCTV equipment also avoids many other problems we have faced, such as parts being unavailable from the manufacturer, or the camera being too costly to repair. In addition, older cameras lose their ability to provide high-quality video and require more maintenance to keep them working.

This request will also benefit from technological changes and improved features of digital cameras that produce much higher quality images than the old-fashioned analog and first-generation IP cameras. Currently, around 18 percent of the cameras in use at Con Ed are older analog cameras and the rest are more modern and clearer IP cameras. The average lifespan of an IP based camera is 5-7 years, which is a concern since this program started in 2014. The plan is to request that this program be ongoing to keep up with the current replacement cycle.

The Company has completed the upgrade of an older Video Management System (VMS) that was no longer supported by the end-of-life software. The new VMS has advanced technology that will enable older analog cameras to be viewed, but with limited functionality. Replacing the end-of-life analog cameras with the newer IP based cameras will allow for full utilization of the technology offered in the cameras, such as video analytics, advanced video compression ratios, full control of multi sensors and a much better picture.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act:

The program life cycle should be ongoing because of the many cameras and the constant changes in CCTV technology. The life span of a camera is only five to seven years. The main goal is to replace all the old analog cameras within the next one to two years (2024-2025). After that, the first IP-based cameras installed will be reaching their end of life. If this program is not continued, there is a danger of cameras breaking down, which would create a security gap. Regularly upgrading the cameras reduces the risk of having obsolete, failing technology. All the Company's facilities would suffer from not keeping up with the CCTV equipment.

2. Supplemental Information

Alternatives

Alternative 1 description and reason for rejection

An option of keeping with the end-of -life analog cameras as well as not staying current on the life cycle of "IP" cameras would eventually result in the loss of CCTV at Company locations, which may also include critical locations throughout the service territory. Loss of such capability would hinder the viewing and confirming that a possible nefarious act was occurring. If such an act were to take place without being able to have a proper response the result could be a disruption of operational services.

Risk of No Action

Risk 1

Cameras will ultimately fail. The resulting loss of video is a vulnerability concern by not having continuous monitoring of our perimeter, access points and assets. In addition, required maintenance/repair costs would be incurred and if the situation could not be immediately resolved, may entail increased costs for hiring guards.

Non-Financial Benefits

Maintaining continuous video monitoring is a deterrent for a would-be adversary. Having the ability to forensically retrieve video is a necessity to conducting security investigations.

Summary of Financial Benefits and Costs (attach backup)

1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Total cost
$6,168,000

4. Basis for estimate
Amount reflects current camera/ancillary equipment costs and vendor/departmental labor for replacing outdated cameras. This is a continuous program and allows us to take advantage of newer technology, which in some cases allows us to reduce the number of cameras at a site. There are still approximately 300 analog cameras that need to be replaced, and the requested funding will allow this to be accomplished in approximately two to three years while reducing the risk of losing CCTV coverage at vital locations.

5. Conclusion
This ongoing program affords the Company to take advantage of cutting-edge technology to keep company assets secure. As pointed out the older legacy cameras are at the end of life and are no longer available on the open market, which proves to be a detriment to the Company's CCTV system. Another benefit of the newer IP cameras is the integration to the new VMS platform and various intrusion detection systems. Installing the newer IP cameras also will give the advantage of reducing the total number of cameras, lessening the overall footprint of cameras on the system which will likely result in lower maintenance costs.

Project Risks and Mitigation Plan

Risk 1 Mitigation plan

There can be a long lead-time for IP-based replacement cameras, which can risk the project completing on time. Leadtime for equipment related to replacing analog with newer IP based cameras is a primary risk related to completing the project on time. To reduce this risk cameras and related equipment will be preordered and kept in stock to be used accordingly per project.

Technical Evaluation / Analysis
N/A

Project Relationships (if applicable)

The Company-Wide Camera project will play an implemental role and relationship with Corporate Security NVR/DVR Replacement Company Wide Program. Program # PR23288877

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year (O&M Only)	Forecast 2024
O&M						
Regulatory Asset						
Capital	**$953**	**$849**	**$883**	**$1,243**		**$1,200**

2025-2029 Request:

Total Request: $6,168,000

Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M					
Regulatory Asset					
Capital (Total)	**$1,200**	**$1,668**	**$1,500**	**$1,500**	**$1,500**
Labor	**$550**	**$700**	**$700**	**$700**	**$700**
M&S					

Contract Svcs.					
Other	**$450**	**$668**	**$500**	**$500**	**$500**
Overheads	**$200**	**$300**	**$300**	**$300**	**$300**

Corporate Security
2025-2029

1. Project / Program Summary

Type: ☐ Project ☒ Program	**Category: ☒ Capital ☐ O&M ☐ Regulatory Asset**
Work Plan Category: ☐ Regulatory Mandated ☒ Operationally Required ☐ Strategic	
Project/Program Title: Corporate Security Technology and Equipment Enhancement Program	
Project/Program Manager: Perry Cuocci	**Project/Program Number (Level 1): 23288877**
Status: ☐ Initiation/Planning ☐ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date: Ongoing	**Estimated Date in Service: Ongoing**
2026-2029 Funding Request ($9,210) **Capital: $6,210** **O&M: $3,000**	

Work Description:

Note: This program was previously referred to as the Corporate Security NVR and DVR Replacements program.

The Company had over 190 Digital Video Recorders ("DVRs") and Network Video Recorders ("NVRs") recording approx. 2,400 cameras. This program replaces underperforming Video Management Systems (VMS) with a new VMS platform and replaces old DVRs/NVRs with the new VMS. The new Windows Server NVRs have better monitoring options, increased storage capabilities, and the ability to capture high quality video footage from digital cameras. Since these NVRs are operating 365 days per year 24 hours and per day, the life expectancy of a quality security NVR is five to six years under ideal conditions not including temperature and dust control. As a result, they need to be changed on a rotational basis to maintain proper operational standards. This program will allow the implementation of a rotational schedule, so no NVR goes beyond their life expectancy and experiences operational issues. Rotation will be completed by Borough/County with priority given to Tier 1 locations.

Additionally, the Security Operations Center (SOC) must be updated on a continual basis to be able to integrate and communicate with the upgraded VMS, NVRs, and IP Digital Cameras. This replacement / upgrade program will enhance the Company's security footprint and maintain the SOCs ability to effectively monitor and respond to alarms, incidents, and events at over 120 critical/tiered business locations. Corporate Security needs to keep pace with the ever-changing technology, specifically with hardware and software for our security systems. This includes software and cyber security updates allowing for the continued safeguarding of Con Edison property as well as the corporate network. Continuing this program will enhance the overall security of the Company and will also take advantage of current and future technologies as they relate to video management systems and effective monitoring and response. The new VMS platform provides the Company with a wide range of new features including being able to integrate with corporate card access systems. The current card access system is approaching 10 years old and will be receiving a software version upgrade this year. Included in the upgrade will be new cyber security enhancements, and as a result, a complete equipment upgrade (card access panels) or replacement system will be needed. This will enhance the

capabilities of the SOC to monitor door alarms and reduce response time to an alarm and/or event. Under this Program, Con Edison will continue to upgrade its security footprint with the rotational replacements of NVRs and associated equipment at the SOC. Additionally, this program will address the aging card access platform. The current cost of replacing an NVR ranges from $19,000 to $40,000 per NVR, plus the associated internal and vendor labor for installation. The wide range in price is reliant upon how many video feeds/cameras an NVR can process at one time. We currently have over 475 card access panels that will need to be upgraded or replaced. Current cost per panel to upgrade is $3,000 each. Based on these costs, the annual Capital request is $1,500. There will be an annual O&M request of $750,000 to account for service agreement contracts for both the VMS and Card Access Systems as well as additional personnel to support the operational capabilities of all security applications.

Justification Summary:

With the implementation of the new VMS platform, we can expand the security footprint at most company locations by integrating several security systems (access control, CCTV, intrusion detection) that can all be monitored within the VMS application. As the Company invests in industry-standard IP digital cameras, recording and storage of the images on corresponding industry-standard NVRs is necessary. Not replacing the NVRs when they reach their life expectancy will effectively nullify the ability of Con Edison to monitor and respond to alarms and events at over 120 locations. This will also hamper the ability of Con Edison Corporate Security Investigators to monitor and retrieve video remotely during incidents when responding to and investigating company incidents.

The newer NVRs are critical to multiple aspects of Corporate Security's monitoring and response capabilities due to their increased technological capabilities. They include such added benefits as larger storage capacity which is needed for the high-quality IP cameras. They are also constructed to provide redundancy, better performance, and data recovery in the event of a hard drive failure.

As the Company strengthens its electronic security measures, the number of NVRs installed and integrated back to our Security Operations Center continues to grow. These newer NVRs will have better monitoring options, to include intrusion detection analytic software as well as alarm notification capabilities, increasing Corporate Security's capabilities for effective monitoring. This makes good business sense as a quality video system is the most critical piece of any monitoring and security system, enhancing the department's ability to further investigative leads through forensic video analysis.

NVRs have multiple purposes: asset protection from theft, vandalism and sabotage, and providing a measure of safety for our employees. The replacement of the end-of-life hardware avoids many other potential issues such as avoiding the VMS from losing connection to the Con Edison SOC, losing the capability to remote monitor for investigations, and losing the enhanced capabilities of Con Edison corporate security to effectively monitor company locations, equipment, and employee safety.

With the current card access platform approaching ten years of age, the associated equipment is reaching its useful end of life. This older equipment is also reaching its useful end of life from a cyber security perspective. With the implementation of our new VMS platform, Corporate Security has enhanced its capabilities of securing critical company locations. This new VMS platform has the ability to intergrate with a variety of robust corporate card access systems. This annual program will allow Corporate Security to better evaluate if the current card access system should be upgraded or replaced.

Upgrading the aging equipment and platforms at the SOC will allow for the utilization of all the enhanced capabilities of the new VMS as well as the new NVRs and IP cameras. These enhanced capabilities such as, video analytics, AI, and SOP management will allow the SOC to function at a

higher level without the need for additional contractors as the security footprint expands. This will keep operational labor costs at the SOC from rising significantly in the future.

Included with platform and system enhancements/upgrades ongoing vendor service/support is critical to maintain these systems/platforms. There is a cost to having vendors provide on going support (service contracts) . An O&M expense has been added to provide for vendor service agreements for our VMS and Card Access systems. Also, an additional ask of an increase in 1 FTE to assist with the operational responsibilities for our Card Access system. With the ever-increasing IT/Cyber standards it is vitally important we are able to address all network connectivity and cyber security issues as they arise.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act:

There is a continued need for this annual program to maintain fully functional security platforms. Providing an annual budget will allow for constant servicing and upgrading of the quickly changing technical security environment. This will provide a cost savings over a period of 5 – 7 years by not having to replace entire systems all at once which would drive up labor and IT costs. In addition, this annual program will allow for the continued adherence to corporate cyber security standards and prevent costly cyber intrusions which has a host of negative impacts to the company and the services it provides.

2. Supplemental Information

Alternatives

Alternative 1 description and reason for rejection

The alternative is to replace NVRs or Card Access Panels/Equipment as they fail. The loss of this equipment for any length of time is a vulnerability concern because it would result in a lack of continuous monitoring of our facilities perimeter, access points and assets.

Risks:

Risk 1 - Fraud
This project will allow us to continue the current processing times, for captured video and card swipe data, which is an ongoing request from our stakeholders and outside partners (Law Enforcement) for investigative purposes.

Risk 2 – Physical Security
Deter and detect safety incidents, as well, use previous safety incident footage to prevent future incidents

Risk 3 – No Action
Waiting for NVRs or Card Access Panels/Equipment to fail before being removed from the corporate network is not a proactive strategy. Many times, a technical piece of equipment (i.e., Workstations, NVRs etc.) are out of cyber security compliance before they physically fail. Often these devices are no longer capable of being upgraded and need to be replaced to stay in line with current corporate standards. In addition, waiting for the devices to fail entails a response which could result in loss of

video, or the inability to monitor live video, until the repair or replacement is scheduled and completed. This puts our employees and assets at risk if an incident were to occur at a location without operational equipment. In addition, aging equipment will require maintenance/repair, and if repair issues could not be immediately resolved, may entail increased costs for hiring guards.

Non-Financial Benefits

Maintaining a corporate security platform that allows for continuous monitoring is a deterrent for a would-be adversary. Having the ability to forensically retrieve and analyze data including video is beneficial to conducting security investigations. CCTV surveillance is a valuable tool in physical security; the loss of equipment prevents surveillance of company assets. Replacing aging equipment and software enables Corporate Security and our internal customers to properly secure Company assets.

Summary of Financial Benefits and Costs (attach backup)

1. Cost-benefit analysis (if required)
As equipment maintenance costs continue to rise, using newer equipment would lower maintenance costs by reducing the amount of maintenance needed to keep our system operational. Reduced equipment down time will eliminate the need to hire physical guards until the equipment is repaired, which will also result in cost avoidance. Maintaining the equipment will also help reduce cyber security intrusions which again will result in a cost savings of having to address a cyber intrusion and the possibility of fines.

2. Major financial benefits

3.Total cost
Next Four Years Est. $6,210 Capital + $3,000 O&M= Total Cost $9,210

4. Basis for estimate
1,500.0 annual Capital request over the next four years and a 750.00 annual O&M request starting in 2026.

Amount reflects the equipment/ancillary costs and vendor/departmental labor for replacing outdated security and network equipment. This will be a continuous program and will allow us to take advantage of newer technology. In some cases, we can reduce the amount of equipment at a location, as an example we once had 190 older NVRs and after replacement now have 128. The amount also reflects an annual service contract with our VMS and Card Access Vendors, along with one additional FTE .

5. Conclusion
This Program should continue as security of Company locations remains a priority in both securing our facilities and personnel, as well as complying with government/industry regulations.

Project Risks and Mitigation Plan

Risk 1 License compliance Mitigation plan Work with legal and supply chain on negotiating terms and conditions for licenses to be used in the dev and test environments

Any issues or delays in the project role out will be managed on a case by case basis and mitigated through manual locks and/or increased human security (guards).
Technical Evaluation / Analysis N/A
Project Relationships (if applicable) Will coordinate with the Corporate Security – Company Wide Camera Rollout Program when necessary

3. Funding Detail ($000)

Historic Spend

	Actual 2020	**Actual 2021**	**Actual 2022**	**Actual 2023**	**Test Year (O&M Only)**	**Forecast 2024**
O&M						
Regulatory Asset						
Capital	822.3	1,500	1,500	0	0	1,500

2025-2029 Request:

Total Request 6,168:

Total Request by Year:

	2025	**2026 (RY1)**	**2027 (RY2)**	**2028 (RY3)**	**2029**
O&M		$750	$75	$750	$750
Regulatory Asset					
Capital (Total)	$1,500.0	$1,710	$1,500	$1,500	$1,500
Labor	$300.0	$400	$400	$400	$400
M&S					
Contract Svcs.					
Other	$1,200.0	$1,310	$1,100	$1,100	$1,100
Overheads					

Corporate Security
2025-2029

1. Project / Program Summary

Type: ☐ Project ☒ Program	**Category: ☒ Capital ☐ O&M ☐ Regulatory Asset**
Work Plan Category: ☐ Regulatory Mandated ☐ Operationally Required ☒ Strategic	
Project/Program Title: Corporate Security – Perimeter Enhancement Program	
Project/Program Manager: Sean O'Connor	**Project/Program Number (Level 1): 25543568**
Status: ☐ Initiation/Planning ☐ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date: January 2026	**Estimated Date In Service: Ongoing Program**
2025-2029 Funding Request ($000) **Capital: $15,000** **O&M:**	

Work Description:

This project will replace existing security fencing Redacted to help keep vital Company assets secure. In 2015 Corporate Security adopted a recommendation to use Redacted at all Company locations. Currently most Company locations are secured by a Redacted

Installation of Redacted poses different challenges based on the location such as: building codes, soil conditions, and underground obstructions. Due to the different variations of size and length of fencing needed at each location it is anticipated that it could take a year or more to complete some locations. These variables in cost and resources will factor in to how many locations will be completed each year. This program would include all work necessary to complete each location, *e.g.,* drawing design packages, engineering, civil work, permits, purchasing material, and all associated labor.

Justification Summary:

Redacted has several benefits:

- Fencing acts as a first line of defense against any breaches or sabotage. The Company's use of a multi-layer security strategy is in line with the security concept of delaying, detecting, and responding to a nefarious act. This multi-layer approach often depends on several electronic driven portions of the security layer, *e.g.,* closed-circuit television surveillance ("CCTV"), Card Access, and Intrusion Detection Systems in addition to a more secure and robust fencing.

- Appearance – Redacted has an appearance of being well built and impenetrable, this can lead to a person with nefarious intent to move on to another more easily accessible location.

- The longer cut through times of Redacted permits more time for a response from Company forces and/or Law Enforcement to cease an intrusion. Older fencing can be cut through in a short amount of time (seconds to minutes) by using commonly available tools while cutting a high security fence can take more than 10 to 20 times as long using power tools.

- Difficult to Climb – the design of the Redacted makes it difficult for a person to grip with their hands and/or feet. This design leads to it taking more effort and time to climb. Again, giving more time for a response to an attempted breach.

- Redacted is designed, engineered, and built with long lasting robust materials which increases the lifespan of the fence. The Redacted that will be installed under this program are manufactured with a powder coating which produces a long-lasting product. Most manufactures place a thirty-to-forty-year lifespan on the fences which would result in significant return on investment.

- Since adopting and installing the standard of using High Security Fencing throughout several Company locations there have been no breaches at these respective sites.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act

Redacted

2. Supplemental Information

Alternatives

Alternative 1 description and reason for rejection
Not replacing the existing fencing that is at most locations throughout the Company. This option could result in a security breach as well as becoming a safety risk.

Alternative 2 description and reason for rejection
Replace existing fencing with traditional 2″ X 2″ or 1″ X 1″ mesh fencing (i.e., chain link fence). This option is not considered security rated fencing and is not an acceptable option due to the standard fencing not providing a good security posture.

Risk of No Action

Not updating and/or upgrading the fencing to Redacted affords a continual risk of not keeping the Company's assets safe and secure. Several times at various Company locations the current older outdated fencing has been easily defeated by people and illegal entry was gained. In most cases a theft or attempted theft occurred. Should one of these perpetrators have had worse intentions the results could have been a loss of operational equipment. The anti-cut/climb fence would be a stronger layer of defense of such acts.

Waiting for the current older outdated fencing to deteriorate and become unrepairable could result in an injury should the fence fall over. Some of the older fencing has been in place over 20 years and were not built as per the same specifications as in the current climate. Taking into consideration wind loads, ice storms and opacity, new updated Redacted designed and engineered to mitigate these occurrences.

Non-Financial Benefits

Redacted will give the Company a more robust security posture, keeping Company employees and assets safe. This fencing visually sends a message to perpetrators as well as the public that the Company takes security seriously and is willing to invest accordingly.

Summary of Financial Benefits and Costs (attach backup)
1. Cost-benefit analysis (if required)

2. Major financial benefits
N/A

3. Total cost
$15,000,000

4. Basis for estimate

Cost has been determined by using cost metrics from previous projects that took place. The cost per location will vary due to the size differential as well as conditions relevant to each location.
Notable Projects for Comparison:

- LNG Plant - $7.5 Million, 4,600 Linear Feet
- Eastview Substation - $3.2 Million. 2,700 Linear Feet
- Corona Substation - $5 Million, 3,600 Linear Feet

5. Conclusion

This project will play a crucial role in keeping Company locations secure. It will also keep the Company up with industry standards and changing atmospheres in security platforms. Benefits of installing Redacted will help mitigate the risks of unwanted entries into Company locations which will keep the risk of interrupting services to customers low.

Project Risks and Mitigation Plan

Risk 1
Lead time for acquiring equipment and material related to installing anti-cut/climb fencing.

Mitigation plan
Advanced planning and proper project management will encourage limiting lead time issues.

Risk 2
Most if not, all digging performed for the fence posts will be hand dug. This process is mandatory for most locations due to underground obstructions that are present at Company locations. Issues with soil being removed from digging could potentially delay and/or halt the project from being completed at a particular location.

Mitigation plan
Proper planning and allowing for the added labor necessary will help mitigate this risk. Working closely with engineers and Environmental Health and Safety will ensure this risk is identified and mitigated prior to specific project commencing.

Technical Evaluation / Analysis
N/A

Project Relationships (if applicable)
N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2021	Actual 2022	Actual 2023	Actual 2024	Test Year* (O&M Only)	Forecast 2025
O&M						
Regulatory Asset						
Capital			$100	$3,500		$3,000

2025-2029 Request:
Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M					
Regulatory Asset					
Capital (Total)	$3,000	$3,000	$3,000	$3,000	$3,000
Labor	$1,500	$1,500	$1,500	$1,500	$1,500
M&S	$600	$600	$600	$600	$600
Contract Svcs.	$200	$200	$200	$200	$200
Other	$400	$400	$400	$400	$400
Overheads	$300	$300	$300	$300	$300

*The test year runs from 10/1/2023 to 9/30/2024

Corporate Security
2025-2029

1. Project / Program Summary

Type: ☐ Project ☒ Program	**Category: ☒ Capital ☒ O&M ☐ Regulatory Asset**
Work Plan Category: ☐ Regulatory Mandated ☒ Operationally Required ☒ Strategic	
Project/Program Title: Protective Intelligence & Countermeasures Program	
Project/Program Manager: Nicholas Boshears	**Project/Program Number (Level 1): 27721709**
Status: ☒ Initiation/Planning ☐ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date: January 1, 2025	**Estimated Date In Service: March 1, 2026**
2025-2029 Funding Request ($25.3M) **Capital: $21.77M** **O&M: $3.55M**	

Work Description:

The objective of this program is to strengthen the ability of Corprate Security to deter, detect, delay, and defend people, assets, and sensitive information from adversaries. The overall program consists of three projects which will enable Corporate Security to meet the objective, exceed NERC/TSA guidelines and requirements while setting conditions to meet ISO standards relevant to security. Redacted

- Redacted

Neptune, Sherman Creek facilities), and cameras to monitor guard attentiveness.

The Protective Intelligence & Countermeasures Program will directly support the request submitted by Con Edison in October 2023 for a DoE sponsored Facility Clearance Level (FCL). To obtain an FCL, Con Edison must meet requirements set forth in the ICD 705, National Industrial Security Operating

Manual (NISPOM) which includes increased physical security and access/visitor controls, additional intrusion detection, an insider threat program, and a DCSA approved space.

This overall program supports compliance with NERC CIP-014-3 and the reasonable and prudent actions recommended by DHS/CISA/OBP, Executive Order 13920, and ISO Standards 22341, 22342, 22361, 27001, 28000, 28001, and 31030.

Justification Summary:

Historically, rate case submissions focused on the physical security aspects whereas this submission considers an enterprise-wide, proactive approach involving all of the other security disciplines – personnel, operational, and information. While cybersecurity remains a significant and increasing threat, the convergence of physical security measures has not experienced the same pace of funding support while counterintelligence and other security risk mitigation measures need to be implemented to more completely safeguard people, IT, OT, and other assets from internal and external threats to include Nation State Actors. As a result, there is a critical need to strengthen and expand the use of proactive measures to deter, detect, and delay criminal, terrorist, and insider acts while simultaneously improving the ability to defend people and protect critical assets to ensure delivery of services. Although this program encompasses significant projects, it is fair, reasonable, and prudent in light of an increased threat to critical infrastructure in the most targeted metropolitan area in the United States.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act

- This program supports Company efforts to reduce Greenhouse Emissions through the use of technology to remotely monitor facilities using solar technology and use hybrid-electric vehicles to reduce the carbon footprint while proactively protecting people and assets which are not covered by video surveillance.

- This program positively benefits Disadvantaged Communities (DACs) as there will be increased engagement across DACs through visible presence and collaboration with the commodities as they perform work in the service territory. Implementation of this program will enable Corporate Security to more efficiently and effectively protect people, information, and facilities to reduce the risk of service disruption and provide support to restore service and maintain continuity of operations. Implementation of RAM will increase the visibility and perception of how the Company prioritizes the protection of the people and facilities which deliver services to their community and not just at large, prominent locations.

- This program supports the Con Edison Clean Energy Commitment Pillar 1/Initiative 1 by ensuring the security of employees and assets associated with building an electric grid, to include clean energy hubs and the continued protection of those systems and facilities to maintain continuity of operations; Initiative 5 by ensuring the security of transmission assets; and Initiative 6 by ensuring the security of energy storage assets. Pillar 3/Initiative 5 is supported by ensuring the security of energy storage assets and hydrogen technologies.

- By protecting people and assets, daily operations can continue uninterrupted which further achievement of the 5-10 year plans.

- This program supports Corporate Instruction 610-4, "Climate Change Resilience and Adaptation Plan", through methodical and professional support to protect people and assets engaged in new construction efforts while working to reduce risk. In the 2024 Office of the Director of National

Intelligence Annual Threat Assessment, the report states, "the risks to U.S. national security interests are increasing as the physical effects of climate and environmental change intersect with geopolitical tension and vulnerabilities of some global systems."

- This program addresses Company risk mitigation activity by promoting a safe work environment, protecting assets, preserving shareholder confidence and market value by mitigating physical and reputational risk.
- This program directly supports company plans to obtain a DoE Facility Clearance Level designation by the DCSA.

2. Supplemental Information

Alternatives

Redacted

Redacted

are intended to augment a full-time program in order to not detract from their full-time positions.

Risk of No Action

Redacted

Redacted

Redacted

Non-Financial Benefits

- Increased safety, reliability, resilience (including climate adaptation), and efficiency
- Improved workflows and communication among departments
- Stronger relationships with community, government, and regulators
- Ensuring regulatory compliance
- Increased public and employee confidence in company to deliver reliable service

Summary of Financial Benefits and Costs (attach backup)

1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits

Redacted

3. Basis for estimate

Capital is based on initial estimates provided by facilities and relevant manufacturers. Present Value to be determined upon receipt of actual amounts per category.

O&M is based on the total of current salary, compensation, and benefits. Present Value to be determined upon receipt of actual amounts per category.

Project Risks and Mitigation Plan

Facilities projects (FCL space, windows, badging office) may incur cost increases and potential cost overruns due to changes in cost of labor, supply chain delays, landmark trade costs, and construction materials pricing.

Risk 1 FCL space	Mitigation plan – Downgrade from Open to Closed Storage Secret.
Risk 2 Window replacement	Mitigation plan - Replace windows to "shatter resistant."
Risk 3 Badging office	Mitigation plan – Change glass in office to "No Entry."

Technical Evaluation / Analysis

In comparison to 2022, physical attacks doubled on critical infrastructure in 2023. In 2023, the Congressional Research Service identified the NERC physical security standards are not enough to

deter a criminal or terrorist from damaging critical infrastructure, particularly the electrical grid and distribution unit substations, causing service outages/disruptions which negatively impact communities.

In the 2024 RAND Corporation Research Report – *Threats to Critical Infrastructure*, two key findings included, "Hesitancy by private organizations to share details about specific threats or threat actors often stems from concerns regarding customer confidence, legal liabilities, or proprietary technology; this hinders information-sharing efforts, planning, response, recovery, and collaboration between affected entities and other stakeholders….Infrastructure protection often requires a deep understanding of targeted infrastructure; highly trained individuals are needed to address these mitigations at the system level and work with other sector experts on cross-sector impacts."

A separate 2023 Congressional Research Service report on pipeline security highlights the need for security measures beyond those required by the TSA. The 2024 DHS Homeland Threat Assessment expects the threat of violence from domestic extremists to remain high while domestic and foreign adversaries likely will continue to threaten the integrity of US critical infrastructure. The 2024 Office of the Director of National Intelligence Annual Threat Assessment states, "U.S. persons and interests at home and abroad will face an ideologically diverse threat from terrorism. This threat is mostly likely to manifest in small cells or individuals inspired by foreign terrorist organizations and violent extremist ideologies to conduct attacks, and the transnational racially or ethnically motivated violent extremists (RMVE) movement, in particular motivated by white supremacy, will continue to foment violence. The loose structure of transnational RMVE organizations and networks, which encourage or inspire but do not typically direct attacks, will challenge local security services and creates resilience against disruptions." The RMVE plot targeting the electric grid supplying Baltimore, which was disrupted in 2024, is a recent example of the need to implement this program.

As of May 2024, the E-ISAC continues to observe elevated levels of serious incidents leading to grid impacts. Between 2022 and 2023, the E-ISAC received over 5,000 incidents of which 3% of those incidents led to grid impacts. Of those incidents that led to grid impacts, the tactics involved were the result of ballistic damage, theft, intrusion and vandalism.

Since 2022, ballistic damage incidents have increased by 58%, and theft incidents have increased by 41%. The E-ISAC assesses with medium to high confidence 55% of incidents that led to grid impacts in 2023 indicated sabotage. The E-ISAC noted online extremists continue to circulate threatening rhetoric and share publications promoting the sabotage of electrical assets.

The National Counterintelligence and Security Center Insider Threat Mitigation for Critical Infrastructure Entities advises, "…it is imperative that critical infrastructure entities prioritize and dedicate resources to preempt and/or mitigate insider threats."

The 2024 National Counterintelligence Strategy states, "Foreign Intelligence Entities (sic) are laying the groundwork for potential attacks against our critical energy, communications, transportation, and financial nodes. Their capabilities and pre-positioning efforts are increasing the risk of a large-scale disruption during periods of conflict or tension, which could include degraded military readiness, major economic losses, loss of life, or eroded confidence in key institutions...a primary goal of the US Government is to, "Facilitate information sharing and data integration across government and with the private sector to gain deeper insight into interdependencies between sectors, vulnerabilities, and threats from FIE and insiders to our most critical infrastructure."

The National Counterintelligence Security Center reported in August 2024, "The US is facing threats from foreign intelligence entities that are unprecedented in their breadth, volume, sophistication, and impact…The exploitation of key U.S. supply chains by foreign adversaries, especially when executed

in concert with cyber intrusions and insider threat activities, represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure."

The 2025 DHS Homeland Security Assessment states, "Over the next year, the terrorism threat environment in the Homeland will remain high. We are particularly concerned about a confluence of factors this year…Domestic and foreign adversaries almost certainly will continue to threaten the integrity of our critical infrastructure with disruptive and destructive cyber and physical attacks, in part, because they perceive targeting these sectors will have cascading impacts on US industries and our standard of living. The PRC, Russia, and Iran will remain the most pressing foreign threats to our critical infrastructure."

The primary Con Edison building, which serves as the Corporate Headquarters, is located at 4 Irving Place in the NYPD Manhattan South Patrol Borough, 13th Precinct, and is approximately one block from Union Square, the site of numerous protests and significant civil unrest. As of May 2024, the NYPD reported 623 violent crimes in the 13th Precinct area.

Project Relationships (if applicable)

This project complements a Facilities improvement effort at 4 Irving Place and other ongoing security projects from prior Rate Case years.

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year (O&M Only)	Forecast 2024
O&M	0	0	0	0		
Regulatory Asset						
Capital	0	0	0	0		

2025-2029 Request:
Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	$350	$4,064	$1,674	$2,793	
Regulatory Asset					
Capital (Total)		$5,520	$4,800	$9,250	$2,200
Labor					
M&S					
Contract Svcs.					
Other					
Overheads					

Facilities & Field Services
2025-2029

1. Project / Program Summary

Type: ☐ **Project** ☒ **Program**	**Category:** ☒ **Capital** ☐ **O&M** ☐ **Regulatory Asset**
Work Plan Category: ☐ **Regulatory Mandated** ☒ **Operationally Required** ☐ **Strategic**	
Project/Program Title: Facility Security Upgrades	
Project/Program Manager: Leo Palmer	**Project/Program Number (Level 1): 22093063**
Status: ☒ **Initiation/Planning** ☐ **In-Progress (Projects Only)** ☐ **On-going (Programs Only)**	
Estimated Start Date: Ongoing	**Estimated Date In Service: Ongoing**
2025-2029 Funding Request ($000) **Capital: $16,500** **O&M:**	

Work Description:

The Facilities Security Program will include upgrade/enhancements to various facilities buildings and yards. The current Plan includes:

Justification Summary:

The Company has improved its security technology over the past several years.

Defense is a critical part of our overall security posture. Replacing a falling fence with new, high security perimeter protection such as the anti-cut, anti-climb fence increases our ability to deter, detect, and delay intruders at our facilities.

Cameras and access control countermeasures safeguard the facilities' assets and keep our employees safe. With cameras and access control, we can assess potential threats in real-time, at each facility for local and remote response. These cameras will come back to the 24/7 Security Operations Center.

These facilities need improvements to the means to control ingress/egress, provide real-time and forensic video footage, provide a hardened perimeter, and thwart any external threats.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act

Con Edison recognizes that climate is changing and considers that the floodplain will extend over time due to sea-level rise, and that temperature and rainfall amounts will also rise. As such facilities will be designed in accordance with standards for climate adaptation. Engineering will design systems in accordance with Climate Change Planning and Design Guideline Document & Corporate Instruction CI-610-4. The specific project will determine which climate change pathways ("the Pathways") and design elements to incorporate into the project for increased precipitation, temperature rise, and sea level rise; the design work scope will apply the "Pathway" for the decadal time horizon associated the specific project. Note that each project and application will need to be reviewed and analyzed.

2. Supplemental Information

Alternatives

Alternative 1 description and reason for rejection
On a cost-effective basis, an integrated access control and camera system provides the most effective deployment of a robust security system at all locations requiring increased security. Access control restricts access to only those authorized to enter, and when it is integrated with a camera system it can provide verification. As an alternative to these measures extensive, around-the-clock guard deployment would be required.

Alternative 2 description and reason for rejection
Depending on the selected climate pathway, the structure and associated facilities will be designed accordingly. Structures that are not in the existing FEMA 100-year floodplain could be built to a lower DFE. Within the useful life of these assets, however, the flood plain is expected to extend to this location. If this alternative is selected, this facility would be vulnerable to damage from future flooding. That would result in an inability to use the facility and disruptions to operations. The incremental cost of planning to a higher DFE is outweighed by the risk of disrupting operations during future storm events and the cost of repairing water damage to the facility.

Risk of No Action

Risk 1
Without action, these facilities will be vulnerable to internal or external threats.

Non-Financial Benefits

These measures will significantly enhance employee safety and security.
The DFE of the facility helps maintain continuous operations during emergency storm events.

Summary of Financial Benefits and Costs (attach backup)
1. Cost benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Basis for estimate
The estimates are developed based on historic knowledge and engineering estimates from previous similar projects for each recommended location. The projected estimates capture construction contract services, and costs associated with internal project management, construction oversight, Facilities/EH&S support, escalation, Company overheads, and contingency.

Project Risks and Mitigation Plan

N/A

Technical Evaluation / Analysis

This security system will provide state-of-the-art security and safety at these company locations. The Company will benefit from centralized monitoring and data management functions, which integrate access control, video surveillance, and fire and burglar alarm systems. The expected results are increased efficiency at a lower cost. System integration will help Con Edison to respond more quickly to potential security threats.

Detailed engineering and architectural analysis have identified the least-cost and best fit design to meet the required DFE.

Project Relationships (if applicable)

N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year* (O&M Only)	Forecast 2024
O&M						
Regulatory Asset						
Capital	$1,458	$2,949	$117	$241		$200

2025-2029 Request:

Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M					
Regulatory Asset					
Capital (Total)	$3,500	$4,000	$3,000	$3,000	$3,000
Labor					

M&S					
Contract Svcs.	$2,816	$3,222	$2,416	$2,416	$2,416
Other					
Overheads	$684	$778	$584	$584	$584

*The test year runs from 10/1/2023 to 9/30/2024

Central Operations / SSO
2025-2029

1. Project / Program Summary

Type: ☐ **Project** ☒ **Program**	**Category:** ☒ **Capital** ☐ **O&M** ☐ **Regulatory Asset**
Work Plan Category: ☐ **Regulatory Mandated** ☒ **Operationally Required** ☐ **Strategic**	
Project/Program Title: Substations Security Enhancements Program	
Project/Program Manager: John Mazzani	**Project/Program Number (Level 1):** 10030235
Status: ☐ **Initiation/Planning** ☐ **In-Progress (Projects Only)** ☒ **On-going (Programs Only)**	
Estimated Start Date: N/A	**Estimated Date In Service:** On-going
2025-2029 Funding Request ($000) **Capital:** $47,300 **O&M:**	

Work Description:
This program is required to systematically upgrade substation security systems throughout New York City's five boroughs and Westchester, Rockland, and Dutchess Counties. Security upgrades include the installation of fencing, surveillance system, access control systems and perimeter intrusion detection systems.

The Company is currently working on security upgrades at Redacted For 2026 to 2029, the Company's goal is to continue to install security upgrades for Transmission/Switching/Area Substations and public utility station (PURS) facilities in priority order. The schedules and prioritization are subject to change based on available funding and coordination with other capital work

A high-level schedule for the planned work is shown below:

	2025	2026	2027	2028	2029
Redacted					

Justification Summary:
The security upgrades are necessary to address the threat of sabotage or terrorism, vandalism, theft, and unauthorized access to the substations per the requirements of Con Edison Security Specification CE-ES-2002-24. The sabotage/terrorism incidents at Moore County, North Carolina substation in December 2022 in which several transformers were damaged by gun fire in a well-coordinated attack that left of over 40,000 people without power for days as well as attacks on substations in the Tacoma,

Washington area also in December 2022, underscore the importance of installing state of the art security systems at the Company's substations. The Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to develop reliability standards requiring owners and operators of the bulk power system to address risks due to physical security threats and vulnerabilities, such as these. This program aligns with the FERC directive, Reliability Standards for Physical Security Measure (CIP-014 Physical Security and CIP-006 Cyber Security and Physical Security of BES (Bulk Energy System) Cyber Systems) to protect critical systems in the substation.

In addition, this work is in accordance with the recommendations made by the Public Service Commission with regards to having security measures in place to enhance protection and increase deterrence of attacks against Con Edison's facilities.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
This program does not directly impact greenhouse gas emissions.

This program upgrades substations across the Con Edison service territory, to include in disadvantaged communities.

This program provides risk mitigation and supports the Company's mission to provide safe, reliable energy to our customers by addressing the Substation Operations Departmental Risk for Safety systematically upgrade substation security systems throughout New York City's five boroughs and Westchester, Rockland, and Dutchess Counties. Security upgrades include the installation of fencing, surveillance system, access control systems and perimeter intrusion detection systems as well as the probability connected to the corporate risk of loss of a substation for more than 24 hours.

This program is a core investment that enables the Company to continue to provide safe and reliable service, even as the nature of the grid changes. This aligns with Con Edison's strategic objective of providing world-class safety, reliability, and security, while managing the equity challenges of the energy transition.

This program is a resilience investment that strengthens utility infrastructure to withstand non-climate related threats and hazards. This aligns with Con Edison's strategic objective to increase resilience of our energy infrastructure to address other hazards and vulnerabilities, such as cybersecurity threats and physical security vulnerabilities.

2. Supplemental Information

Alternatives
The only alternative to making the proposed investments is to do nothing and accept the risks of security systems failing and opening up vulnerabilities – including potential damages/failures to connected or near-by equipment - and potential customer outages. Replacing failed security equipment under emergent or emergency conditions (such as during or after storms) may require expedited measures that require the Company to incur additional costs compared to planned upgrades or replacements, and the impact of resulting outages on customers may also be more significant in emergency situations.

Risk of No Action
Taking no action is not a recommended approach as these security enhancements are necessary to address regulatory requirements concerning physical security threats to electric power facilities. These

upgrades provide substation facilities with protection against the threat of vandalism, theft, and security breaches. These acts have the potential to compromise electric service to our customers and increase the risk to the safety of the public and Company personnel. Undertaking this program will also comply with Con Edison Security Specification CE-ES-2002-24 as well as the associated regulatory requirements.

Non-Financial Benefits
This program supports the coordinated effort between government agencies and utilities to protect against physical security threats to the nation's power facilities. This program provides risk mitigation and supports the Company's mission to provide safe, reliable energy to our customers.

Summary of Financial Benefits and Costs (attach backup)
1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
A significant security incident would result in a substantial cost for the Company to respond to the emergency and implement recovery efforts.

3. Basis for estimate
The annual funding request of $10M is based on a 5-year historical average.

Project Risks and Mitigation Plan
Risk 1: Lack of alignment between resources support

Mitigation Plan 1: Anticipate, schedule, and pre-plan with resource requirements such as engineering, labor, and construction to avoid alignment conflicts with scheduling.

Technical Evaluation / Analysis
The measures to be deployed have been reviewed with/by the Company's security experts.

Project Relationships (if applicable)
N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year* (O&M Only)	Forecast 2024
O&M	$0	$0	$0	$0	$0	$0
Regulatory Asset	$0	$0	$0	$0	N/A	$0
Capital	10,000	10,000	10,000	15,000	N/A	12,000

2025-2029 Request:
Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	$0	$0	$0	$0	$0
Regulatory Asset	$0	$0	$0	$0	$0
Capital (Total)	$7,000	$10,000	$10,000	$10,000	$10,300
Labor	$1,740	$2,646	$2,646	$2,646	$2,646
M&S	$1,680	$1,100	$1,100	$1,100	$1,325
Contract Svcs.	$1,400	$3,200	$3,200	$3,200	$3,200
Other	$70	$100	$100	$100	$100
Overheads	$2,110	$2,954	$2,954	$2,954	$3,028

*The test year runs from 10/1/2023 to 9/30/2024

Central Operations / S&TO

2025-2029

1. Project / Program Summary

Type: ☐ **Project** ☒ **Program**	**Category:** ☒ **Capital** ☒ **O&M** ☐ **Regulatory Asset**
Work Plan Category: ☒ **Regulatory Mandated** ☒ **Operationally Required** ☐ **Strategic**	
Project/Program Title: Energy Control Center's (ECC & AECC) Security Enhancements	
Project/Program Manager: Christopher Minix	**Project/Program Number (Level 1):** 22950477
Status: ☐ **Initiation/Planning** ☐ **In-Progress (Projects Only)** ☒ **On-going (Programs Only)**	
Estimated Start Date: Ongoing	**Estimated Date In Service:** 12/31/2029
2025-2029 Funding Request ($000) **Capital:** $16,285 **O&M: $1,121**	

Work Description:

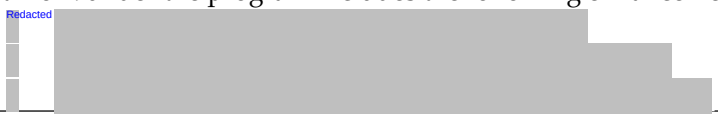
The uninterrupted operation of the Energy Control Center (ECC) and the Alternate Energy Control Center (AECC) is essential for maintaining the reliable and safe operation of the Bulk Electric System (BES) and Steam System. The control centers have always maintained a level of security appropriate to the critical nature of the activities performed within the centers. Continued improvements to maintain a high level of security are needed to support our operational needs. In addition, compliance with regulatory requirements (the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards, New York State Reliability Council (NYSRC), Northeast Power Coordinating Council, Inc. (NPCC), is mandatory for critical facilities like the control centers. Failure to comply with these regulatory requirements can subject the Company to significant monetary penalties as great as $1.25 million per violation per day, as well as damage to its reputation.

This project replaces the battery system for at the Energy Control Center uninterrupted power supply (UPS) systems that provide protection and uninterrupted transfer of load to the emergency diesel generators by the three 80kva UPS systems and the associated Transfer Switches.

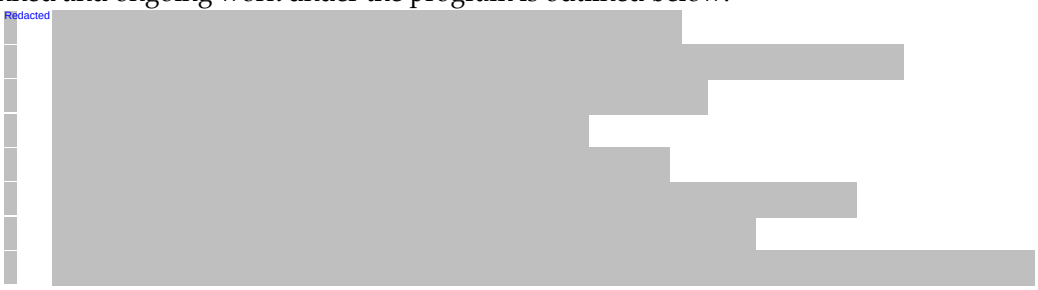
These projects will add new and improved physical security systems to the two control centers – ECC and AECC. This will include two FTEs to work on items such as card access, video analytics, security cameras, cUAS (Counter Uncrewed Aircraft Systems) – Drone Detection Equipment , Biometrics screening systems, Network Video Recorder (NVR) systems , intrusion detection systems, Uninterrupted Power Supply (UPS) for security systems, physical Access Point (PSP) upgrade/replacement and new PSP, emergency evacuation systems, anti-piggybacking access portals, intercom systems, duress (panic) systems/applications, Chemical and Biological Detection system (CBR), and other automated applications to monitor security in order to maintain and improve the overall security of the control center and to address emergent security needs.

Past work under the program includes the following enhancements:

Redacted



Planned and ongoing work under the program is outlined below:



Outlined below is the cost breakdown for planned activities:

Activity	Cost	Planned Duration
Work activity #1	$864,340	24 months
Work activity #2	$3,695,593	36 months
Work activity #3	$2,336,052	48 months
Work activity #4	$2,938,052	48 months
Work activity #5	$2,300,590	60 months
Work activity #6	$2,700,590	60 months
Work activity #7	$2,240,590	60 months
Work activity #8	$2,895,000	24 Months

The additional O&M cost is for equipment repairs, compliance testing that is a regulatory requirement e.g. NERC CIP-006., psychological evaluation, increase in guard services that was required after a CIP-006 Potential Non-Compliance, and other physical security tasks that have increased over time.

Justification Summary:
The control centers provide an essential service, each having full control capability of the electric and steam systems. Physical security systems must be maintained at levels that provide proper access control and allow for both local and remote monitoring. In addition, NERC policies require specific levels of physical security for critical cyber locations, which this project will address as necessary. Additional security enhancements will be needed to keep up with emergent NERC CIP requirements and security threats.

In order to continue to improve internal security and access control within the control centers, frequent evaluations of our security systems are needed, as are enhancements such as additional card access points, cameras, intrusion detection systems, and others. These new components will be installed at locations within the facilities in order to improve the monitoring capability and security posture within the control centers in general and the Physical Security Perimeters (PSPs), in particular. The enhancement of the communications capability with the Security Operations Center (SOC) is another goal of this project.

The critical systems at the Energy Control Center are protected by three 80kva UPS systems. The critical systems require battery support to provide protection and to allow uninterrupted transfer of load to the emergency diesel generators. This project will replace the battery systems for our UPS systems. The batteries will be replaced while the critical load is transferred to a temporary battery system, to ensure continued operation of the critical computer systems.

The security upgrades and enhancements as outlined above will assist the ECC and the AECC in conforming to NERC CIP requirements as well as hardening the overall security infrastructure in the facilities. Failure to meet regulatory requirements may subject the Company to fines upward of $1.25 million per day, per violation.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
This program is related to the Physical Security Risk. The projects associated with this program will mitigate some of the FERC and NERC regulatory compliance and physical security risks faced by System Operation.

This program will enhance security of the ECC and AECC, which benefits the entire Con Edison service territory, to include in disadvantaged communities.

This program is a core investment that enables the Company to continue to provide safe and reliable service, even as the nature of the grid changes. This aligns with Con Edison's strategic objective of providing world-class safety, reliability, and security, while managing the equity challenges of the energy transition.

This program is a resilience investment that strengthens utility infrastructure to withstand non-climate related threats and hazards. This aligns with Con Edison's strategic objective to increase resilience of our energy infrastructure to address other hazards and vulnerabilities, such as cybersecurity threats and physical security vulnerabilities.

2. Supplemental Information

Alternatives
Alternative 1: An alternative would be to not to commit to this project in its entirity at the ECC and/or AECC
Reason for Rejection:

Alternative 2:The battery systems for the ECC UPS systems are approaching the manufacturer 15-year age limit and must be replaced for protection and uninterrupted transfer of load to the emergency diesel generators in the event of a loss of power.

Reason for rejection: This alternative is rejected because it would cause the ECC to fall out of compliance with the NERC Critical Infrastructure Protection (CIP) Standards, and to deal with existing and emergent security threats. If the Company does not meet regulatory requirements, it may face fines of up to $1.25 million per day, per violation.

Risk of No Action
Risk 1: The Company could be found to be out of compliance with the NERC CIP Standards. Financial penalties for non-compliance can be up to $1.25 million per day, per violation, per day, and the Company could sustain reputational damage as well.

Risk 2: Failure to invest in security improvements may increase the likelihood of a successful attack on the control centers(s), which could result in the loss of key personnel and property and may significantly impair the Company's ability to operate the electric and steam systems.

Risk 3: The UPS battery systems will not provide support during power outages, scheduled feeder outages or emergency diesel tests. Without battery support, computer equipment would shut down during any type of loss of power, interrupting operability, and potentially corrupting data files. Failure of no UPS system battery protection would place the Energy Control Center in non-compliance for Northeast Power Community Counsel (NPCC) directory 8 regulatory requirements.

Non-Financial Benefits

- Improve the security of the control centers while helping to ensure compliance with the NERC CIP regulatory requirements.
- Assist in conforming to regulatory requirements such as NERC CIP, which can prevent substantial fines for non-compliance.
- Increase customer and employee protection, reducing the possibility of system and building intrusion.
- Support compliance with various security standards and executive orders and ensuring holistic security involving personnel, operational, and information disciplines.
- Provide power protection and uninterrupted transfer of load to the diesel generators due to a loss of power at the Energy Control Center.

Summary of Financial Benefits and Costs (attach backup)

1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
The major financial benefit is loss avoidance. Losses can come from penalties associated with NERC compliance violations, or attacks on either of the two control centers that result in the loss of life, plant, property, or equipment. Enhancements such as additional card access points, cameras, and intrusion detection systems not only improve security but also help in conforming to NERC CIP requirements. Non-compliance with these requirements could result in fines of up to $1.25 million per day, per violation, thus, compliance saves a substantial amount of money.
The ECC and AECC house high, medium, and low impact BES Cyber Systems, which is crucial for maintaining the reliability of the Bulk Electric System. The physical security indirectly contributes to financial benefits by ensuring system reliability and preventing costly outages or disruptions. Prevention of potentially damaged Energy Control Center critical computer equipment due to the loss of power and transfer of load on an emergency diesel generator.

3. Basis for estimate
The table below shows the actual costs for 2020-2023 and some of the 2024 cost. The historical and forecasted cost show the ramping of systems/hardware aging. This results in an increase cost as system come to end of life. Postponing upgrades would put the security of the Energy Control Centers at risk of critical failures and potential compliance violations.

Sum of Actual Dollars	2020	2021	2022	2023	2024	Grand Total
22947782-L0_ECC FACILITY SECURITY ENHANCEMENT	$ 317,563.57	$ 403,728.99	$ 449,949.66	$ 19,128.22		$ 1,190,370.44
Accounts Payable	$ 288,858.48	$ 326,735.88	$ 419,488.18	$ 18,499.40		$ 1,053,581.94

Allocated Cost Labor			$ 449.62			$ 449.62
Allocated Cost Non Labor			$ 210.75			$ 210.75
Burden Cost Labor	$ 3,113.88	$ 4,676.07	$ 5,286.24	$ 236.32		$ 13,312.51
Burden Cost Non Labor	$ 6,788.59	$ 28,861.25	$ 13,223.35	$ 392.50		$ 49,265.69
Contract Services			$ 544.95			$ 544.95
Labor	$ 3,230.17	$ 41,674.21	$ 9,898.85			$ 54,803.23
Other	$ 15,572.45	$ 1,781.58	$ 847.72			$ 18,201.75
26975992-L0_ECC/AECC FACILITY SECURITY ENHANCEMENTS				$ 4,517,257.74	$ 237,571.74	$ 4,754,829.48
Accounts Payable				$ 4,194,033.28	$ 153,363.93	$ 4,347,397.21
Burden Cost Labor				$ 35,318.37	$ 2,404.13	$ 37,722.50
Burden Cost Non Labor				$ 137,441.80	$ 23,660.65	$ 161,102.45
Labor				$ 150,464.29	$ 58,143.03	$ 208,607.32

The basis for estimate is based on the previous battery replacements and quote from the vendor.

Project Risks and Mitigation Plan

Risk 1: Current staffing levels are insufficient to support timely program implementation
Mitigation plan: Compliance/QA is hiring new analysts for the Compliance and Security Team.

Risk 2: Delays associated with understanding how certain projects can affect our NERC compliance program

Risk 3 - Project timeline extensions risk due to Bulk Electric System (BES) operating conditions and the inability to proceed with the battery system replacement.
Mitigation plan – All operators and needed staff work from the Alternate Energy Control Center (AECC) during the project.

Risk 4 - Prevent Completion Risk - UPS Battery protection is unavailable due to the installation of the new battery string. Critical load is not protected in the event of a loss of power.

Mitigation plan 1: Bi-weekly meetings are held between the Compliance and Security Team and the Infrastructure and Cyber Security Team to review the status of planned and on-going security projects, and to discuss any compliance concerns

Mitigation plan 2: Connect a temporary battery string to provide protection for critical load during the removal of the old batteries and the installation of the new batteries.

Technical Evaluation / Analysis

Con Edison routinely benchmark with other Bulk Power Operators to identify new technologies that can improve our security and NERC CIP-006 compliance posture. While at the same time we are member of multiple forums to include North American Transmission Forum (NATF), Electric Power

Research Institute (EPRI), and Association for Uncrewed Vehicle System International (AUVSI). We also review practices with National Defense agencies and Homeland Security.

Energy Control Center physical security upgrades are essential for maintaining the reliability and security of the bulk power system. These upgrades are closely aligned with NERC CIP-006 and CIP-014 standards.

Physical Security Plans (CIP-006): Projects often involve developing and implementing comprehensive physical security plans. These plans include measures to control access to critical cyber assets, such as secure access points, surveillance systems, and intrusion detection.

Risk Assessment and Refinement (CIP-014): NERC has ongoing projects to refine risk assessments for physical security. These projects aim to improve methodologies for identifying and mitigating risks to critical infrastructure, ensuring that control centers are adequately protected.

Access Control and Monitoring (CIP-006): Upgrades typically include enhanced access control systems and continuous monitoring of physical access points. This helps in detecting and responding to unauthorized access attempts, thereby protecting critical cyber assets.

Stakeholder Engagement (CIP-014): NERC emphasizes robust stakeholder engagement to ensure that physical security measures are effective and practical. This involves collaboration with industry experts, government agencies, and other stakeholders to develop and refine security standards.

Implementation of Advanced Security Technologies (CIP-006 & CIP-014): Projects often involve the deployment of advanced security technologies such as biometric access controls, high-resolution surveillance cameras, and automated intrusion detection systems. These technologies enhance the physical security of control centers.

Compliance and Continuous Improvement (CIP-006 & CIP-014): Entities are required to regularly review and update their physical security plans and risk assessments. This ensures ongoing compliance with NERC standards and continuous improvement in security measures.

These relationships highlight the interconnected nature of physical security upgrades and NERC standards, ensuring that Energy Control Centers remain resilient against physical threats.

The replacement of the UPS battery systems was recommended by the manufacturer due to the maximum 15-year age limit. Maintaining the battery system over the 15-year limit will cause the batteries to fail and not provide protection to the critical computer systems.

Project Relationships (if applicable)
This program is to provide for the physical security of the control centers and cyber assets covered by the Cyber Security, Infrastructure, and NERC Compliance program. While ensuring all security system allow Bulk Power Operators, District Operators, and supporting staff to perform their duties without any hindrance

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year* (O&M Only)	Forecast 2024
O&M						
Regulatory Asset	$0	$0	$0	$0	N/A	$0
Capital	$ 318	$ 404	$450	$4,500	N/A	$ 2,100

2025-2029 Request:
Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M		$$247	$287	$287	$300.00
Regulatory Asset	$0	$0	$0	$0	$0
Capital (Total)	$2,240	$4,619	$2,336	$3,908	$3,182
Labor	$867	$305	$313	$568	$325
M&S	$0	$3,588	$1,500	$2050	$2,244
Contract Svcs.	$930	$306	$310	$848	$324
Other	$0	$0	$0	$0	$0
Overheads	$443	$420	$213	$442	$289

*The test year runs from 10/1/2023 to 9/30/2024

Central Operations / S&TO
2025-2029

1. Project / Program Summary

Type: ☒ **Project** ☐ **Program**	**Category:** ☒ **Capital** ☐ **O&M** ☐ **Regulatory Asset**
Work Plan Category: ☐ **Regulatory Mandated** ☒ **Operationally Required** ☐ **Strategic**	
Project/Program Title: Energy Control Center (ECC) Relocation	
Project/Program Manager: Dennis Holmes	**Project/Program Number (Level 1):** 27727675
Status: ☒ **Initiation/Planning** ☐ **In-Progress (Projects Only)** ☐ **On-going (Programs Only)**	
Estimated Start Date: January 2026	**Estimated Date In Service:** May 2032
2025-2029 Funding Request ($000) **Capital:** $470,000 **O&M:**	

Work Description:
The objective of this work is to relocate the existing Energy Control Center to a location that conforms with modern industry standards for physical security and create a workspace that utilizes modern technology to support the transition to the clean energy future. In support of this objective, this project will establish the Transmission & Renewable Energy Control Center which will serve as the primary operational control center for the bulk electric transmission system and the steam system. This includes the installation of the Energy Management System along with all required control room equipment and subsystems required to reliably monitor and operate both systems. This will include additional equipment and staffing workstations required to visualize, monitor, and analyze wind farms, transmission level battery systems and other forms of renewable energy projects on the bulk electric system.

This project will be sited at a location in Westchester that will provide a physical security barrier from pedestrians and vehicles that is consistent with modern best industry practices and also taking into account the ability to eliminate the overflight of line of site controlled unmanned aerial vehicles (i.e. drones).

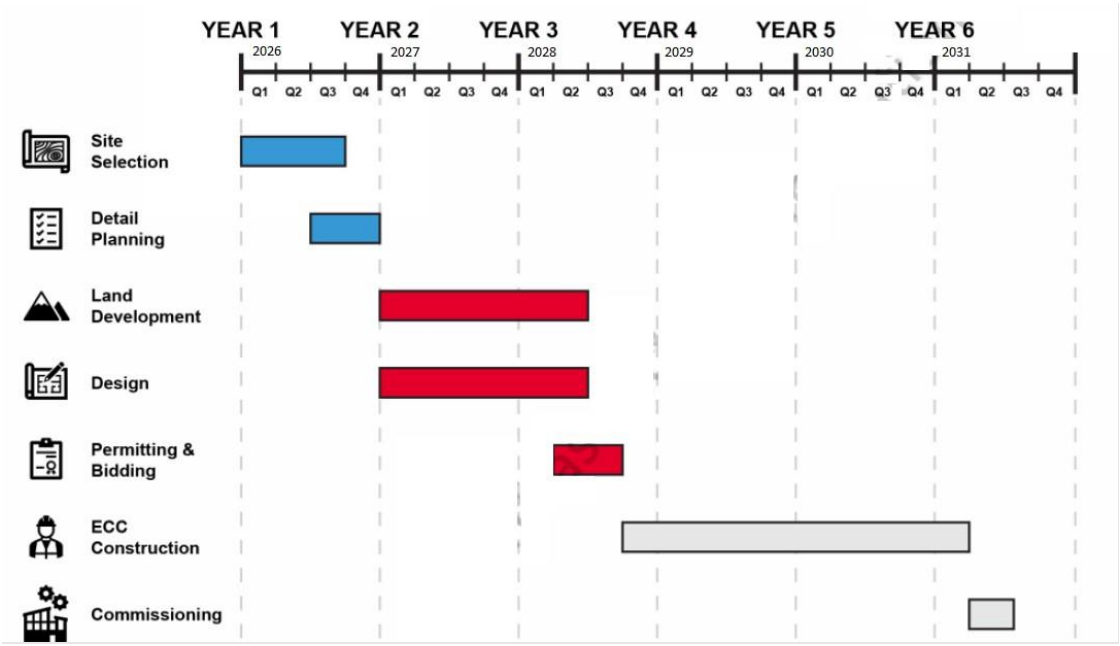
The project will be designed and constructed to meet the latest industry standards for an energy control center. A state-of-the-art security system and building management system for HVAC and fire protection systems will be employed. A reliable and redundant Light and Power supply with diesel generators as backup and UPS support system for critical loads will also be included to ensure the safe and reliable operation of both the bulk electric system and steam system.

Major work components include:

- Site Selection: Identify and secure property (20-40 acres)
- Detail Planning: Conduct detailed project planning based on site selection
- Land Development: Prepare site for construction
- Design: Engineer and design a structure conforming with latest industry best practices for physical security and reliable operation of the transmission system

- Permitting & Bidding: Appropriately permit the work and put the project out for contractor bid
- ECC Construction: Construct the new building and security perimeter
- Commissioning: Obtain NPCC certification of the new facility

This project requires land acquisition in 2026, with engineering and long lead equipment procurement to begin in 2027 for this project. The in-service date of this project is May 2032. A high-level schedule is shown below:



Justification Summary:

Redacted

In 2019, New York State passed the nation-leading Climate Leadership and Community Protection Act (CLCPA). To achieve the ambitious goals set by the CLCPA requires a transformation in the way power is generated, interconnected, and utilized by customers. One of the CLCPA requirements is to interconnect 9,000 MW of Offshore Wind (OSW) by 2035. Along with a large influx of clean energy projects with growing electrification needs, this project will be sized to incorporate the necessary

building infrastructure to manage the increased control center staffing and operational requirements needed to reliably monitor and control the growing bulk electric transmission system.

The new Energy Control Center will include a new 140,000 square foot facility, which will also include control room spaces for the Security Operation Center (SOC), Advanced Metering Infrastructure (AMI) Operations and Cyber Security Operations (CSO) Centers. The existing control rooms for the SOC and AMI will serve as their alternate locations, while CSO will use the new location as their alternate.

The new Energy Control Center is expected to contain sufficient space for approximately 275 employees within the following teams:

System Operations – Responsible for the 24/7 reliable operation and coordination of the bulk electric system including all transmission equipment and inter-utility tie lines. Provides protection for work on both the electric transmission and distribution systems. Responsible for the reliable operation and coordination of the Con Edison steam system. Make notifications to various local, state, and federal agencies with respect to the status of the electric, steam and gas systems.

Security Operation Center (SOC) - Responsible for the 24/7 physical and electronic security at all non-NERC CIP Con Edison facilities. Monitor camera feeds and respond to alerts from the Physical Access Control System (PACS). Company locations are monitored by video feeds from the cameras and are viewed live via the workstations and stored on the DVR servers for future investigations, while physical access is monitored via a card reader and sensors on the door. The card reader system records badge usage and can alert on several conditions (for example, forced door or propped door). In addition, the SOC receives security calls from employees and the public. The SOC operators can dispatch investigators to follow up, as necessary.

Advanced Metering Infrastructure (AMI) Operations – Responsible for the 24/7 monitoring and control of the advanced meter infrastructure ("smart meters"). Customer turn on/turn off can also be performed.

Cyber Security Operations (CSO) Center – Responsible for the 24/7 basis to support four major cyber related functions: alert triage, intelligence, threat hunting, and incident response. Con Edison has deployed several security tools which collect data and generate alerts, all of which are monitored by CSO personnel. These systems have visibility into corporate IT devices, including the corporate physical access infrastructure and some non-NERC CIP OT infrastructure. The CSO owns and maintains an Operational Playbook, as well as part of the incident response function. The CSO contacts and dispatches cyber forensics resources and determines initial mitigations.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act

The system improvements implemented with this project would be sufficient to mitigate control center physical security risks and ensure the bulk electric and steam systems remain capable of satisfying reliability, resiliency, safety, and compliance regulations.

This project does not directly impact greenhouse gas emissions.

This project will relocate the ECC, which supports the entire Con Edison service territory, to include disadvantaged communities.

This project is a core investment that enables the Company to continue to provide safe and reliable service, even as the nature of the grid changes. This aligns with Con Edison's strategic objective of

providing world-class safety, reliability, and security, while managing the equity challenges of the energy transition.

This project is a resilience investment that strengthens utility infrastructure to withstand non-climate related threats and hazards. This aligns with Con Edison's strategic objective to increase resilience of our energy infrastructure to address other hazards and vulnerabilities, such as cybersecurity threats and physical security vulnerabilities. This project would directly address and mitigate the physical security risks associated with the existing Energy Control Center. The existing building is located over a substation, does not meet recommend standoff distances for physical security, does not allow for the planned future growth, and does not provide protection from an EMP event, explosion, and other catastrophic man-made or natural threats. For these reasons, major improvements and upgrades would be required to be made to protect the facility and bring it in-line with Industry Best Practices. The impact of these improvements would be limited and extremely difficult, if not impossible, and costly to implement within an existing facility.

2. Supplemental Information

Alternatives
Alternative 1: Remodel the existing energy control center.

Reason for rejection: The feasibility of this alternative would need to be studied. The existing building dimensions would limit the ability to create new workspaces to accommodate additional operators and support staff. The HVAC and Communication infrastructure would need to be modernized and properly diversified, if this is even possible due to the nature of its original design. This alternative would also not be able to address the physical security, electromagnetic pulse, and overhead security concerns.

Alternative 2: Retrofit space within the Con Edison headquarters at Irving Place or at one of the existing Company-owned properties.

Reason for rejection: The location at Irving Place is not ideal since the headquarters are in a high traffic area of Manhattan and would be a vulnerable, high-risk target in terms of security concerns. Additionally, the existing Company-owned properties do not offer ample space to site a new facility to contain the necessary resources and required security measures.

Risk of No Action
Risk 1: If this project is not pursued, the existing physical security vulnerabilities will remain in place and the ability of the operators to efficiently and reliably operate the bulk electric transmission system will be diminished.

Non-Financial Benefits
Provides the necessary reliability and resiliency to monitor and operate the bulk electric system in an area that serves many critical loads (e.g., airports, transportation hubs, and hospitals) in a densely populated area where many buildings have elevators and various equipment loads.

Summary of Financial Benefits and Costs (attach backup)
1. Cost-benefit analysis (if required)

N/A

2. Major financial benefits
N/A

3. Basis for estimate
The conceptual estimate was developed using construction costs from similar construction projects by peer utilities. Our vendor, Robert E Lamb (REL), had construction data from seven projects constructed recently or currently under construction. The projects cited did not include land acquisition, IT infrastructure, utility feeders to the site, Con Edison direct/indirect costs, environmental remediation, and escalation. As such, REL's order of magnitude cost was rolled into a standard Company estimate form to capture missing cost, such as IT infrastructure, internal Company labor (e.g., project management, construction inspection, facilities support, IT/security/EH&S oversight), escalation, Company overheads, and contingency. Direct costs are estimated to be $458 million including all services for the design, construction and installation of support systems within the building. This includes the $100 million for the two data centers was based on the costs of recent company IT projects. This may have extra contingency money being assigned but it should not be double counting the escalation. 21% escalation was applied along with a 30% contingency budget.

Project Risks and Mitigation Plan
Risk 1: The land acquisition process takes longer than expected, resulting in project schedule delays.

Mitigation plan 1: As soon as funding is available, the Company intends to hire a real estate broker to support and help expedite the land acquisition process.

Risk 2: Building materials have lead times longer than originally planned for, resulting in schedule delays.

Mitigation plan 2: The Company intends to stay abreast of industry-wide lead times and prioritize orders for long lead time materials (e.g., structural steel, electrical equipment) as early as possible to mitigate the chance for construction schedule delays.

Technical Evaluation / Analysis
Confidential NATF guidance documents were used to develop this project. An architectural firm with extensive experience designing and constructing transmission control centers was retained to provide further guidance on the current industry best practices for the design concepts. This criteria includes, but is not limited to, the following:

Project Relationships (if applicable)
N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year* (O&M Only)	Forecast 2024
O&M	$0	$0	$0	$0	$0	$0
Regulatory Asset	$0	$0	$0	$0	N/A	$0
Capital	$0	$0	$0	$0	N/A	$0

2025-2029 Request:

Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	$0	$0	$0	$0	$0
Regulatory Asset	$0	$0	$0	$0	$0
Capital (Total)	$0	$55,000	$35,000	$180,000	$200,000
Labor	$0	1,587	7,057	38,938	40,913
M&S	$0	$0	$0	$0	$0
Contract Svcs.	$0	5,036	22,399	123,587	129,853
Other	$0	47,585	1,227	6,772	7,115
Overheads	$0	792	4,317	10,703	22,119

*The test year runs from 10/1/2023 to 9/30/2024

Information Technology
2025-2029

1. Project / Program Summary

Type: ☒ Project ☒ Program	**Category: ☒ Capital ☒ O&M ☐ Regulatory Asset**
Work Plan Category: ☒ Regulatory Mandated ☐ Operationally Required ☐ Strategic	
Project/Program Title: Cyber Security Infrastructure (Cyber for High Value Networks (HVN))	
Project/Program Manager: Kurt John (CISO)	**Project/Program Number (Level 1): 23317522**
Status: ☐ Initiation/Planning ☒ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date:	**Estimated Date In Service: Ongoing**
2025-2029 Funding Request ($000) **Capital: $29,366.33** **O&M: $23,594.77**	

Work Description:
Con Edison has a segmented computing system, that is, higher value assets are not in the same area as lower value network. A high value network is a network where critical technology is needed to operate our electric, gas and steam infrastructure across our service area. It is critical for making sure we keep this infrastructure secure and reliable. Like with other projects, the technology in this area is constantly changing and improving, requiring us to continually upgrade and introduce the applicable products. This project aims to bring the next generation applicable security capabilities into our high value network environments and develop a strong security posture for our infrastructure.

The complexity and uniqueness of HVN environments require specialized knowledge and skill sets that differ significantly from traditional IT security. HVN systems are integral to the operation of our critical infrastructure, and any disruption could have severe consequences, including safety risks, operational downtime, and financial losses. We are looking for funding for both projects and full-time employees (FTEs) to staff this program.

In the last few years, this program upgraded our capabilities and infrastructure for HVN:

We must continue to upgrade and improve our protections for these high value networks during the upcoming rate years:

As systems and technology improve, these projects for tools and processes for the HVN environment may be substituted to meet the company's needs.

Staffing:

Employees involved in project implementation will charge their time to capital, while those supporting ongoing program operations will be charged to O&M. Due to overlapping functionalities between this program and the Cybersecurity program, any historic labor O&M spend related to this program is documented in the "Funding Detail Chart" within the Cybersecurity O&M program whitepaper. However, labor specific to this program will be captured from 2026 onwards in the "Funding Detail Chart" for this program.

We are requesting funding and headcount to establish and grow a dedicated security team with expertise in Operational Technology (OT) to have the necessary capabilities to protect these vital systems effectively. As the integration of IT and OT networks has introduced new vulnerabilities and attack vectors, a specialized security team focused on OT will be able to develop and implement tailored security strategies, conduct risk assessments, and deploy advanced threat detection and response capabilities to mitigate these risks. During the upcoming rate years, there is an ask to increase Enterprise Cybersecurity headcount by 20 FTEs to primarily account for working on the HVN aspects of security.

The remaining incremental 46 FTEs that are part of InfoSec's ask are in the companion IT Security (Non-HVN) paper). Specifically for the 20 headcount, the following breakdown applies:

O&M Description:
The O&M for rate years 2026-2028 ($3,421.00 total in rate year one, $5,911.00 total in rate year 2, and $6,504.00 in rate year 3) accounts for the associated O&M (subscription and maintenance costs) from projects implemented prior to the rate years as well as new project implementations during the rate years plus the labor to expand and maintain new tools and processes.

The O&M accounts for the subscription and maintenance tails of previous implementations of the Industrial Control System specific intrusion detection tools, PAM, and deception technology. With new capital implementations, there will be additional O&M for the recurring software and hardware maintenance and support and subscription costs.

Justification Summary:
Cybersecurity is a significant enterprise risk. Cybersecurity requirements for IT systems associated with the company's business operations have continued to grow as the risks and threats of cyber-attacks have increased. We need to keep pace with best practices and an ever-changing market. Regulatory standards are expected to continue to evolve, especially at the federal level. The risk to availability and reliability of the electric systems increases greatly without advanced cyber security capabilities and formal cyber polices to protect these assets. New technologies and enhanced processes (*e.g.*, automation) are needed to mitigate the new risks from file-less malware, supply chain cybersecurity risks, and continually evolving advanced persistent threats.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
Cybersecurity is one of the most significant enterprise risks. This program will help address this corporate risk by enhancing the company's ability to protect its HVN data and assets from cyber threats and mitigate the risk of attacks.

2. Supplemental Information

Alternatives

The alternative option is to operate IT systems as they are today, supported by current technology. This approach will not appropriately protect customer information or defend against new threat vectors and techniques. This option is not recommended as it opens Con Edison to security threats.

Risk of No Action

New security technology is required to prevent unauthorized access to the company's high value networks and safely deliver energy. Failure to address this will place systems at risk and they will be vulnerable to targeted attacks and where regulatory standards are mandated, put the company at risk of incurring fines due to non-compliance.

Non-Financial Benefits
The non-financial benefits include increasing customer and employee information protection(s), reducing the possibility of intrusion into company systems, using resources more efficiently to perform cybersecurity assessments, and reducing the gaps in the current question-answer process.

1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Basis for estimate
Historic purchases are used, as well as vendor presentations and Internet sources. The requested expense for maintenance assumes 20% of the capital spend in each year after the initial purchase of the equipment. As more technologies are subscription based, this percentage increases.

Project Risks and Mitigation Plan

Risk	Mitigation Plan
Resources are unavailable for implementation.	Secure Contractor Resources
Scope Creep	Initial requirement gathering and involving appropriate stakeholders, robust change control process, regular review of project progress

Technical Evaluation / Analysis

IT Security Engineering is dedicated to analyzing new technologies and policies introduced within our organization. In alignment with risks and our IT strategy and vision planning process, we implement cybersecurity solutions, policies and procedures to ensure robust protection and seamless operations. We also engage in interactions with IT advisors, vendors, and company stakeholders to select the most optimal solutions for our needs. This collaborative approach allows us to maintain the goal of staying ahead in the ever-evolving tech landscape and deliver the best outcomes for our company. Based on this approach, we have laid out our plan for the Cyber Security Infrastructure (Cyber for HVN) program.
Project Relationships (if applicable) N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year (O&M Only)	Forecast 2024
O&M	**0**	**241.76**	**517.66**	**1,010.66**	**978.00**	**1,019.00**
Regulatory Asset						
Capital	**1,813.41**	**1,682.35**	**1,818.25**	**4,030.55**		**3,558.78**

2025-2029 Request:

Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	**1,107.765**	**3,421.00**	**5,911.00**	**6,504.00**	**6,651.00**
Regulatory Asset					
Capital (Total)	**2,580.00**	**5,796.77**	**6,911.03**	**6,925.09**	**7,153.43**
Labor	**1,700.00**	**2,000.00**	**2,200.00**	**2,200.00**	**2,200.00**
M&S	**367.48**	**3,193.36**	**4,145.40**	**4,149.94**	**4,400.00**
Contract Svcs.	**600.00**	**800.00**	**800.00**	**800.00**	**800.00**
Other	**(194.16)**	**(436.32)**	**(520.19)**	**(510.85)**	**(542.57)**
Overheads	**106.68**	**239.73**	**285.82**	**286.00**	**296.00**

Information Technology
2025-2029

1. Project / Program Summary

Type: ☒ Project ☒ Program	**Category: ☒ Capital ☒ O&M ☐ Regulatory Asset**
Work Plan Category: ☒ Regulatory Mandated ☐ Operationally Required ☐ Strategic	
Project/Program Title: Cybersecurity	
Project/Program Manager: Kurt John (CISO)	**Project/Program Number (Level 1):** 10025668 and 23321388
Status: ☐ Initiation/Planning ☒ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date: 1/01/2024	**Estimated Date In Service: Ongoing**
2025-2029 Funding Request ($000) **Capital: $80,133.93** **O&M: $210,065.77**	

Work Description:
Cybersecurity is one of the highest risks for organizations, including Con Edison. Cyber-attacks have increasingly targeted critical infrastructure providers, including utilities. Malicious actors have increased their capabilities, and such attacks can cause serious disruption to the operation of the company's corporate Information Technology (IT) network, operational networks, and critical energy infrastructure. Additionally, there are increasing threats targeting sensitive and confidential information inclusive of customer and employee Personal Identifiable Information (PII). The company continues to refine enterprise-wide detailed strategies to identify and mitigate these risks.

Enterprise Cybersecurity is responsible for company-wide cybersecurity policies, procedures, and practices. During the three rate years (2026-2028), Enterprise Cybersecurity will increase cybersecurity capabilities through investments in people, processes, and technology. These projects are enterprise-level and intended to protect company computer systems and information, detect threats and attacks as well as respond to, and recover from cybersecurity incidents.

During the rate years, Con Edison is also looking to expand in a few areas, including our vulnerability management program, inclusive of people, processes, and technology, to better enable the company to quickly respond to vulnerabilities and reduce cybersecurity risk. Vulnerabilities are one of the primary vectors of attacks and actively managing them reduces the likelihood of compromise. Besides vulnerability management, we will be focusing on software security, detection and incident response enhancements, data protection, cloud and network security, and continue to implement life cycle replacements (software and hardware) when necessary.

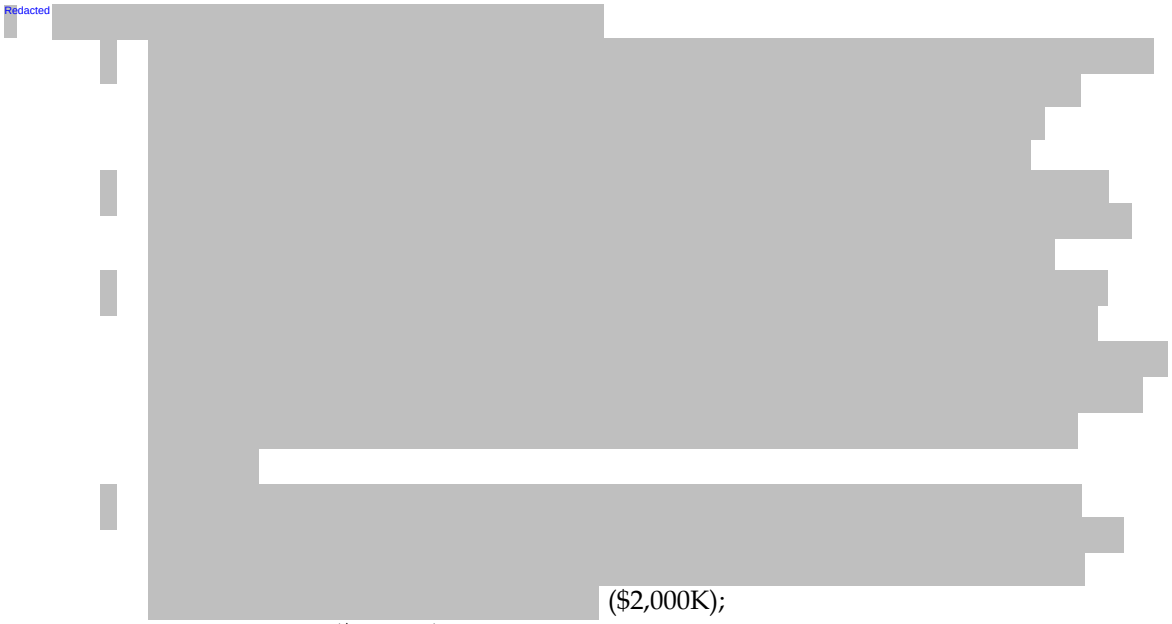
It is also necessary to regularly evaluate and replace hardware and software, so they are up-to-date and capable of mitigating new security risks.

Projects Projected by Year

Set forth below is a list of currently proposed capital projects for the calendar year 2025. However, as systems and technology improve, these projects may be substituted to meet the company's needs.

Set forth below is a list of currently proposed projects for calendar year 2026 (*i.e.*, Rate Year 1). However, as systems and technology improve, these projects may be substituted to meet the company's needs.

Set forth below is a list of currently proposed projects for calendar year 2027 (*i.e.*, Rate Year 2). However, as systems and technology improve, these projects may be substituted to meet the company's needs.



($2,000K);

- Improve PII Protection ($1,000K);

Set forth below is a list of currently proposed projects for calendar year 2028 (i.e., Rate Year 3). However, as systems and technology improve, these projects may be substituted to meet the company's needs.

Note: Building out or enhancing these capabilities includes a combination of hardware, software solution, processes, and professional services, where applicable or necessary.

IT Enterprise Security Operations and Maintenance Work Description
The Cybersecurity plan calls for the implementation of $80.13 million of capital projects over five years ($10.18M in 2025, $17.07M in 2026, $17.18M in 2027, $17.76 M in 2028 and $17.85M in 2029), many of which require annual maintenance or an ongoing subscription costs. The accompanying O&M in the rate years $38.37M in total in rate year 1, $45.48M in total in rate year 2, and $48.45 in rate year 3. Of these amounts, $25.66M in total in rate year 1, $31.71M in total in rate year 2, and $34.06M in rate year 3 for recurring maintenance, subscriptions, and cybersecurity services such as penetration testing. The O&M budget increase is due to the inclusion of new advanced cybersecurity technologies, such as an API Security Management, a Vulnerability Management Aggregation Platform, and Automated Penetration Testing solution. Because more solutions are becoming subscription based, there is a need to account for O&M increases. There is also a need to maintain existing maintenance and subscription contracts from past capital implementations, such as the Virtual Private Network, Data Security solutions, and the Security Information and Event Management (SIEM). To illustrate this, approximately $21.77M of the $25.66M in rate year 1 is for existing maintenance and subscription contracts from past capital implementations, while the remaining amount primarily accounts for the O&M tails (maintenance and subscriptions) from new implementations.

In addition, contractor services are required to continue performing automation of cybersecurity operations and increase the level of threat hunting, penetration testing, and security and vulnerability assessments and remediations.

IT Enterprise Security Organization Staffing
The company proposes an expansion of the IT Enterprise Security organization.

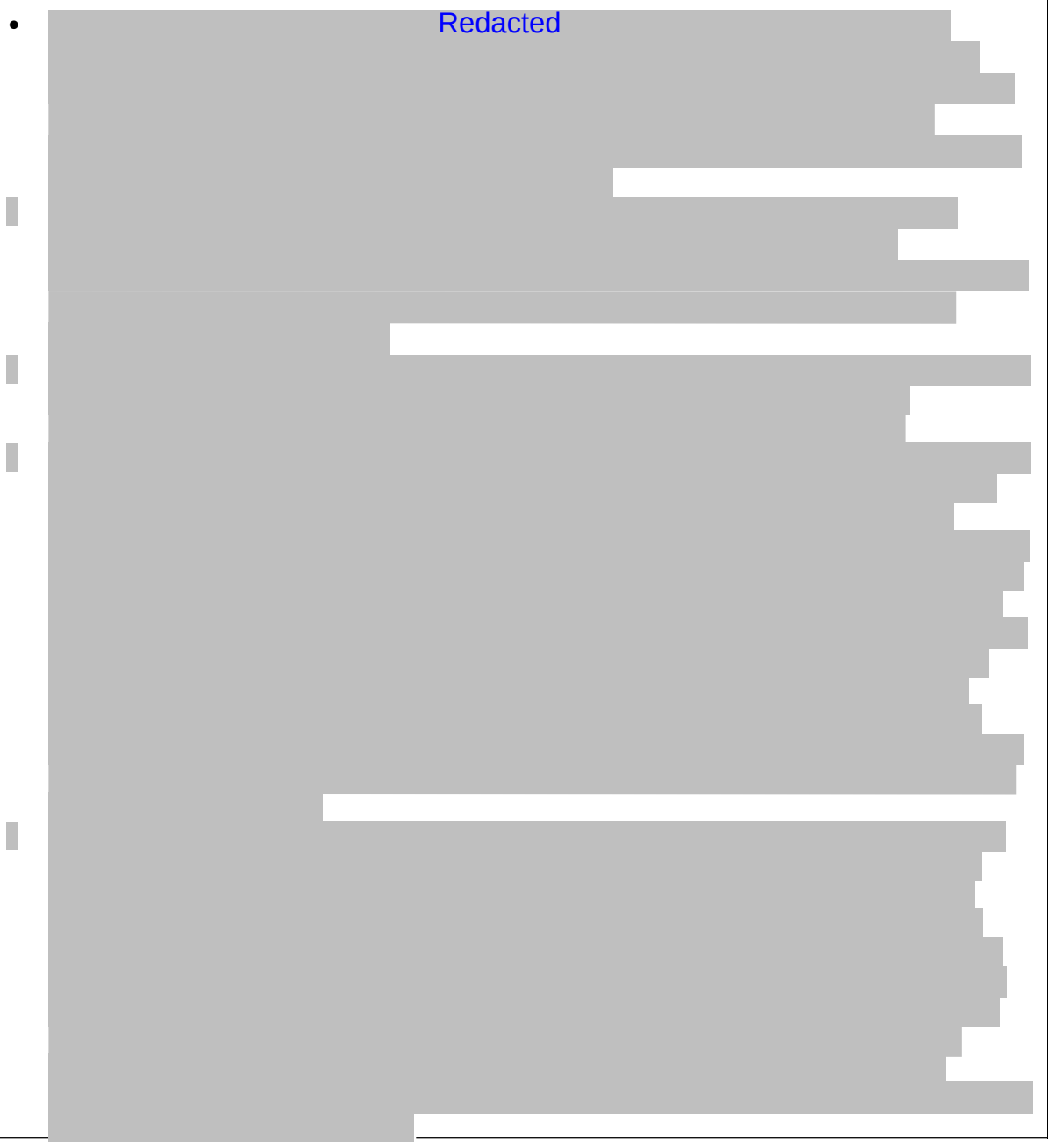
The organizational changes and recurring operational costs will enhance the overall cybersecurity program. As technologies are continuously evolving, operational costs are required to maintain technical skills, manage and support security products (internally and via vendor maintenance

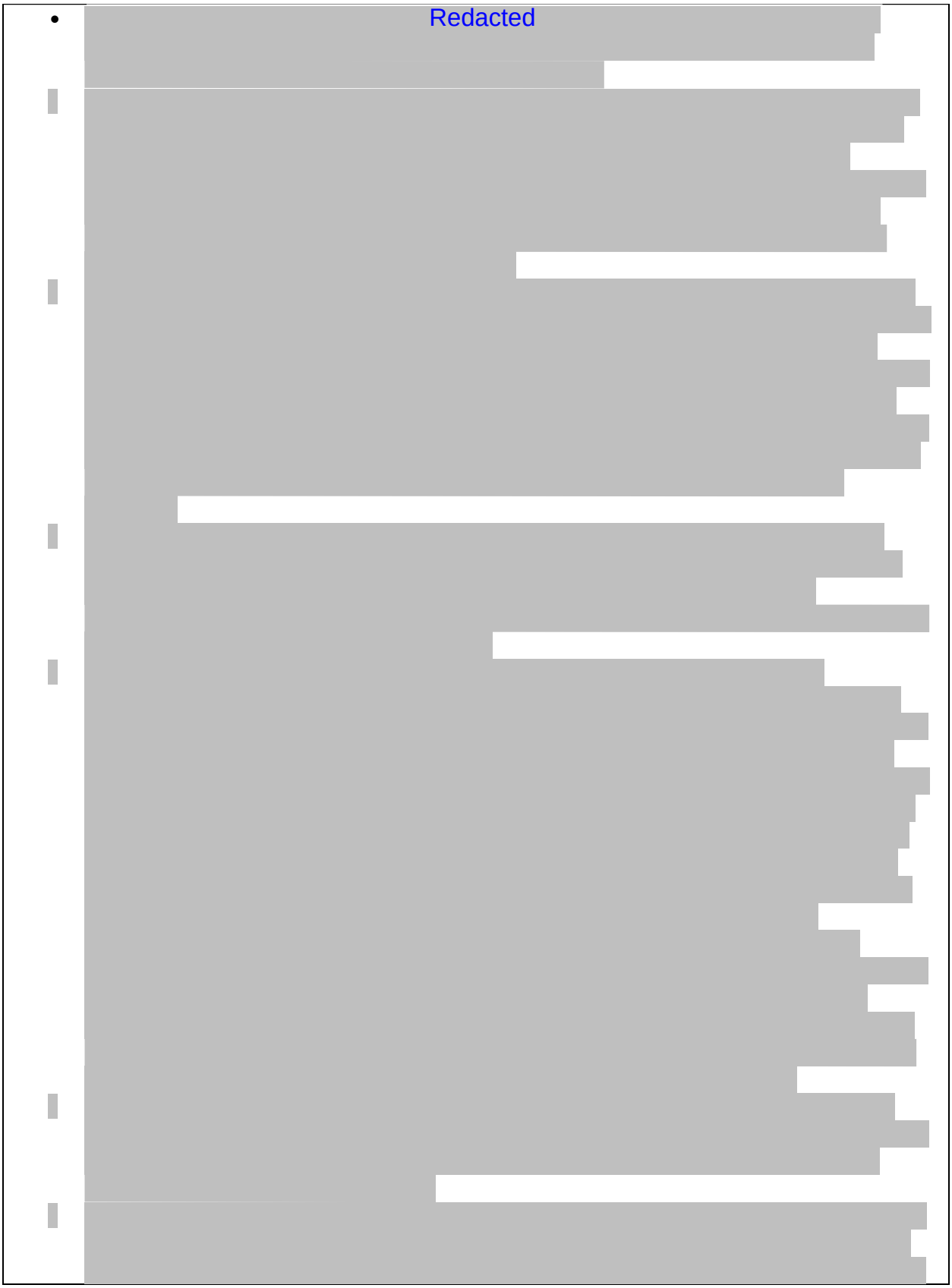
agreements), and enhance risk management, threat management, and compliance capabilities. Costs associated with staffing will provide the necessary skills and knowledge to implement and operate the various cybersecurity programs.

The FTE headcount for Enterprise Security is expected to grow by 66 total (46 under the Cybersecurity program and 20 under the Cyber Security Infrastructure program) over the rate period (including interns). As mentioned, 20 of these new employees are covered under the Cyber Security Infrastructure whitepaper.

The Enterprise Security group is responsible for implementing cybersecurity policy reflecting company policy and applicable regulatory standards.
The growth is attributable to:

- Redacted




Redacted

Redacted

Justification Summary:
Cybersecurity requirements for IT systems associated with the company's business operations have continued to grow as the risks and threats of cyber-attacks have increased. Regulatory standards are expected to continue to evolve, especially at the federal level. The risk to availability and reliability of the electric systems increases greatly without advanced cyber security capabilities, and formal cyber and administrative polices to protect these assets. New technologies and enhanced processes (*e.g.*, automation) are needed to mitigate the new risks from file-less malware, supply chain cybersecurity risks, and continually evolving advanced persistent threats.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
N/A

2. Supplemental Information

Alternatives
The alternative option is to operate the company's IT systems as they are today, supported by current technology. This approach will not appropriately protect customer information or defend against new threat vectors and techniques as threats continue to grow.

Risk of No Action
Risk 1: New security technology is required to continue to protect customer information, prevent unauthorized access, and safely deliver energy. Failure to address this will place systems at risk and they will be vulnerable to targeted attacks and where regulatory standards are mandated, put the company at risk for fines due to non-compliance.

Non-Financial Benefits
This project will allow for improved availability and reliability of current and new systems. Today's technology allows for greater automation, remote control, and data acquisition to help improve efficiencies and allow potential cost reductions associated with these benefits. A support structure will allow more systems to be used, to segregate, secure, and improve energy delivery.

Summary of Financial Benefits and Costs (attach backup)

1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Basis for estimate
Historic purchases are used, as well as vendor presentations and Internet sources. The requested expense for maintenance assumes 20% of the capital spend in each year after the initial purchase of the tool. As more technologies use a subscription model, however, this percentage increases, often to 100% of the initial spend on the subscription after the initial after the initial purchase of the tool.

Project Risks and Mitigation Plan

Evaluate and describe any risks that might extend the project timeline, prevent completion, or lead to cost overruns. Explain plan to minimize these risks.

Risk	Mitigation Plan
The possibility of resources assuming contingency assignments outside of IT presents a risk to the project schedule	Mitigation plan is to identify resources who will be retained by IT to assume responsibility for the work of those who are called to contingency assignments.

Technical Evaluation / Analysis

IT Security Engineering is dedicated to analyzing new technologies and policies introduced within our organization. In alignment with risks and our IT strategy and vision planning process, we implement cybersecurity solutions, policies and procedures to ensure robust protection and seamless operations. We also engage in interactions with IT advisors, vendors, and company stakeholders to select the most optimal solutions for our needs. This collaborative approach allows us to stay ahead in the ever-evolving tech landscape and deliver the best outcomes for our company. Based on this approach, we have laid out our plan for the Cybersecurity program.

Project Relationships (if applicable)

The security processes and tools employed in the corporate environment via this program (Cybersecurity) are evaluated for deployment in High Value Network (HVN) environments. The Cybersecurity Infrastructure program covers the funding for those projects in HVN.

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year (O&M Only)	Forecast 2024
O&M	8,038.00	11,326.59	12,733.87	20,894.25	23,771.00	24,077.63
Regulatory Asset						
Capital	8,290.97	15,141.50	8,739.73	18,493.74		9,798.18

2025-2029 Request:

Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	28,084.73	38,374.00	45,477.00	48,453.00	49,677.04
Regulatory Asset					
Capital (Total)	10,280.87	17,067.70	17,176.00	17,756.32	17,853.04
Labor	4,500.00	4,900.00	5,100.00	5,400.00	5,400.00
M&S	4,961.65	11,538.03	11,450.00	11,750.00	11,850.00
Contract Svcs.	1,200.00	1,200.00	1,200.00	1,200.00	1,200.00
Other	(759.78)	(1,265.85)	(1,274.00)	(1,317.68)	(1,324.96)
Overheads	379.00	695.52	700.00	724.00	728.00

Central Operations / SSO
2025-2029

1. Project / Program Summary

Type: ☐ **Project** ☒ **Program**	**Category:** ☒ **Capital** ☐ **O&M** ☐ **Regulatory Asset**
Work Plan Category: ☒ **Regulatory Mandated** ☒ **Operationally Required** ☐ **Strategic**	
Project/Program Title: NERC Cyber and Physical Security Critical Infrastructure Upgrade	
Project/Program Manager: Arman Shiplu	**Project/Program Number (Level 1):** 10079362
Status: ☒ **Initiation/Planning** ☐ **In-Progress (Projects Only)** ☐ **On-going (Programs Only)**	
Estimated Start Date: January 2025	**Estimated Date In Service:** December 2029
2025-2029 Funding Request ($000) **Capital:** $60,460 **O&M:** $0	

Work Description:
The purpose of this project is to upgrade cyber and physical infrastructure at Company substation facilities to comply with regulatory requirements. This includes installing physical access controls and additional logical controls to meet North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security requirements. Currently, substations utilize serial communications that are not routable to communicate voltage, current and breaker status to the Energy Control Center (ECC). Substations will be upgraded from serial to fiber communications from 2026-2028, to allow for the ECC to be able to trace and resolve issues when they arise.

As result of communication conversion from serial (Time Division Multiplexing - TDM) to fiber communications (Internet Protocol - IP), over 40 additional CIP requirements associated with External Routable Connectivity (ERC) will come into scope. The addition of these requirements has categorized the substations that require cyber and physical infrastructure as medium or low risk. To prepare for this additional scope, the objectives within the rate years include fortifying substation physical security, installing a centralized substation management network, and upgrading two substations with ERC as pilot stations. After the pilot phase, the long-term plan is to continue this work along another 30 substations under NERC CIP compliance in future rate years.

Justification Summary:
This program funds cyber and physical security enhancements that will be implemented in all transmission substation facilities because of North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security requirements. Substation Bulk Electric System (BES) Cyber Assets are critical to the reliable operation of the electric system. Seventy percent of the top 10 most violated NERC are with CIP Cyber Security standards. The substation cyber security program will go through a transformation of its existing processes, procedures, and utilization of technology. This will require capital expenditure to bolster the substation cyber and physical security program to adhere to the additional 40 plus CIP requirements.

Some benefits of ERC include:

- Real time substation network monitoring and data collection, which will help with quicker response and recovery during cyber and electric system events.
- Remotely patch and manage passwords for cyber assets such as network switches and protection relays, rather than physically dispatching crews to each location to perform these functions.
- Facilitates asset management and baseline configuration of cyber assets in real time, which will alert for any deviations.
- Facilitates use of synchronized phasor measurement data for advanced monitoring and protection functions.

All necessary new IT infrastructure will support the substation Operational Technology (OT) environment. This will be tested at two transmission substations prior to full deployment.

The project is designed to streamline the deployment and management of substation assets, ensuring that the process is both efficient and effective. By leveraging advanced technologies and innovative practices, the project aims to reduce the time and resources required to install and maintain these critical components of the electrical grid.

One of the key benefits of the project is its ability to support the electrification of various sectors by providing a reliable and robust infrastructure for the transmission and distribution of clean, renewable electric power. This is achieved through the integration of smart substation assets that can adapt to the dynamic demands of the power grid, facilitating the smooth flow of electricity from renewable sources to consumers.

From 2026 onwards, the forecasted cost to upgrade the cybersecurity and physical infrastructure of the substations has increased due to approximately 40 more requirements being mandated by ERC requirements. Please see additional CIP Requirements below.

ERC Requirements - NEW for SSO	
4.2	**Cyber Security Training Program (Version 7 enforceable in 2024)**
4.2.1	Include training contents <refer to NERC CIP-004 R2.1
4.2.2	Must complete training before authorized electronic access or unescorted physical access
4.2.3	Must complete training every 15 months
4.3	**Personnel Risk Assessment Program (Version 7 enforceable in 2024)**
4.3.1	Process to confirm Identity
4.3.2	Perform 7-year criminal history records check
4.3.3	Evaluate criminal history records for authorizing access
4.3.4	Verify contractors & service vendors go through 3.1-3.3 check
4.3.5	Process to perform Personnel Risk Assessment, within the last seven years according to parts 3.1-3.4 for every employee who have authorized electronic or unescorted physical access
4.4	**Access Management Program (Version 7 enforceable in 2024)**
4.4.1	Process to authorize electronic access, unescorted physical access
4.4.2	Quarterly check that those with access have authorization records (unescorted Physical or active Electronic)
4.4.3	15-month check that electronic access provided to authorized persons only.
4.5	**Access Revocation (Version 7 enforceable in 2024)**

4.5.1	Process to revoke access within 24 hours of termination - interactive remote access & unescorted physical access
4.5.2	Process to revoke unnecessary access for Employee transfers within 24 hours of determination
4.6	**Access Management for BES Cyber System Information (Version 7 enforceable in 2024)**
4.6.1	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 6.1.1. Provisioned electronic access to electronic BCSI; and 6.1.2. Provisioned physical access to physical BCSI.
4.6.2	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.
4.6.3	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI: 6.2.1. have an authorization record; and 6.2.2. still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.
5.1	**Electronic Security Perimeter**
5.1.2	All external routable Connectivity must be through identified EAP (electronic access point)
5.1.3	Require inbound and outbound access permissions for EAPs including the reason for granting access and deny all other access by default.
5.2	**Interactive Remote Access Management**
5.2.1	Ensure Cyber Asset Initiating interactive remote access does not directly access the H/M Cyber Asset/associated PCA
5.2.2	For all interactive Remote Access sessions, utilize encryption that terminates an Intermediate system
5.2.3	For all interactive Remote Access sessions, require multi-factor authentication
5.2.4	Require inbound and outbound access permissions for EAPs including the reason for granting access and deny all other access by default.
5.2.5	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
5.3	**Vendor Remote Access Management for EACMS and PACS**
5.3.1	Have one or more method(s) to determine authenticated vendor-initiated remote connections.
5.3.2	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.
6.1	**Physical Security Plan**
6.1.2	Use at least one physical access control for unescorted physical access - Medium BES Cyber Systems & External Routable Conn.
6.1.4	Monitor for unauthorized access to a Physical Security Perimeter
6.1.5	Issue alarm for detected unauthorized access to Physical Security Perimeter to appropriate personnel within 15 mins
6.1.6	Monitor for unauthorized access to a Physical Access Control system
6.1.7	Issue alarm for detected unauthorized access to PACS to appropriate personnel within 15 mins
6.1.8	Log entry of each individual with authorized unescorted physical access into each Physical Security Perimeter
6.1.9	Retain physical access logs of entry of individuals w authorized unescorted physical access to Physical Security Permit - for 90 days
6.2	**Visitor Control Program**
6.2.1	Require continuous escorted access of visitors w/o authorization for unescorted physical access - except during CIP Exceptional Circumstances
6.2.2	Log visitor entry and exit of Physical Security Perimeter - except during CIP Exceptional Circumstance

6.2.3	Retain visitor logs for 90 days
6.3	**Maintenance and Testing Program**
6.3.1	Maintenance and testing of PACS and locally mounted hardware/devices at Physical Security Perimeter - every two years
7.1	**Ports and Services**
7.1.1	Enable only logical network accessible ports that are needed by the Responsible Entity, IT has firewalls, control system has HMI, switches
7.4.2	Generate alerts for security events that includes detected malicious code, detected failure of logging incident events
7.5	**System Access Controls**
7.5.1	Have a method to enforce authentication of interactive user access
7.5.3	Identify individuals who have authorized access to shared accounts
7.5.6	Enforce password changes every 15 months

In summary, this project plays a pivotal role in the modernization of the electrical grid, enabling the adoption of renewable energy and supporting the global efforts towards a sustainable and clean energy landscape.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
The project emphasizes the importance of sustainability and environmental responsibility. The use of renewable energy sources, coupled with the efficient management of substation assets, contributes to the reduction of greenhouse gas emissions, and promotes the transition to a greener energy future.

This project addresses substations across the Con Edison service territory, including in disadvantaged communities.

This program is a core investment that enables the Company to continue to provide safe and reliable service, even as the nature of the grid changes. This aligns with Con Edison's strategic objective of providing world-class safety, reliability, and security, while managing the equity challenges of the energy transition.

This program is a climate resilience investment that is in line with the New York State Climate Leadership and Community Protection Act (CLCPA). This program helps transition to a clean energy economy, replacing outdated infrastructure and improving system efficiency enhances the grid's capacity for renewables. Upgrading cyber and physical infrastructure reinforces the grid against extreme weather events in support of CLCPA's goals of climate resilience and protecting vulnerable communities.

This program is a resilience investment that strengthens utility infrastructure to withstand non-climate related threats and hazards. This aligns with Con Edison's strategic objective to increase resilience of our energy infrastructure to address other hazards and vulnerabilities, such as cybersecurity threats and physical security vulnerabilities.

2. Supplemental Information

Alternatives
There is no alternative to performing the work, as it is mandated by FERC/NERC. This is a regulatory requirement in order to establish External Routable Connectivity at BES substations. Furthermore,

TDM technology is obsolete and the telephone companies, including Verizon, as well as Con Edison's internal communication infrastructure are moving to an IP based system.

Risk of No Action
Taking no action would leave the BES vulnerable to cyber-attacks. It would also leave the Company subject to substantial fines for failure to comply with a FERC/NERC mandated program. The fines can be up to 1.2 million dollars per violation per day.

Non-Financial Benefits
Business and operational demands for managing and maintaining a reliable BES increasingly rely on BES Cyber Assets supporting critical reliability operating services and processes to communicate with each other, across functions and organizations, for services and data. This program ensures compliance with regulatory mandates (FERC, NERC, NPCC) and addresses Cyber Security corporate Enterprise Risk.

Summary of Financial Benefits and Costs (attach backup)
1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Basis for estimate
The cost estimate is focused over 3 years (2026-2028) for a total $45 million or $15 million per year.

Software – $15 million
Servers (internal to substation network) – $2 million
Data center to support substations - $6 million
Gatekeeper visitor management – $5 million
Contractor resources - $8 million
Create new online training – $1 million
New "NERC" background check – $1 million
Transient Cyber Asset (TCA) laptops – $3 million

Physical security enhancements to protect cyber assets:
New perimeter gate alarm system– $2 million
New Prowatch instance dedicated for substations – $2 million

Project Risks and Mitigation Plan
Risk 1: Delays due resource/support coordination

Mitigation plan 1: Anticipate, schedule and pre-plan with resource requirements such as engineering, labor, and construction and outages to avoid performance delays alignment conflicts.

Risk 2: Material Availability Issues

Mitigation plan 2: Engineering will work with Supply Chain to establish a cohesive plan that aligns with vendor lead times. Stay engaged with vendors to ensure lead times are maintained, and adjust the plan as needed if shortages are encountered.

Technical Evaluation / Analysis

N/A
Project Relationships (if applicable) N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year* (O&M Only)	Forecast 2024
O&M	$0	$0	$0	$0	$0	$0
Regulatory Asset	$0	$0	$0	$0	N/A	$0
Capital	$269	$83	$548	$101	N/A	$639

2025-2029 Request:
Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	$0	$0	$0	$0	$0
Regulatory Asset	$0	$0	$0	$0	$0
Capital (Total)	$460	$15,000	$15,000	$15,000	$15,000
Labor	$0	$2,771	$2,771	$2,771	$2,771
M&S	$166	$1,200	$1,200	$1,200	$1,200
Contract Svcs.	$88	$7,050	$7,050	$7,050	$7,050
Other	$105	$0	$0	$0	$0
Overheads	$102	$3,979	$3,979	$3,979	$3,979

*The test year runs from 10/1/2023 to 9/30/2024

Business Unit / Division
2025-2029

1. Project / Program Summary

Type: ☒ Project ☒ Program	**Category: ☒ Capital ☐ O&M ☐ Regulatory Asset**
Work Plan Category: ☐ Regulatory Mandated ☒ Operationally Required ☐ Strategic	
Project/Program Title: TNVS Web	
Project/Program Manager: Christopher Minix	**Project/Program Number (Level 1):**
Status: ☐ Initiation/Planning ☒ In-Progress (Projects Only) ☐ On-going (Programs Only)	
Estimated Start Date: 2021	**Estimated Date In Service: Dec 31, 2030**
2025-2029 Funding Request ($000) **Capital: 11,500.00** **O&M:**	

Work Description:

Note: A discrepancy was noted in the dollars requested for this program after the revenue requirement was calculated. This will be corrected at update.

The Transmission Network Visualization System (TNVS) is a "Life Boat" system that provides situational awareness used as the backup system for the Energy Management System (EMS). Which is the critical system that provides situational awareness and control for Bulk Power System Operators, District Operators, and Energy Dispatched. The process is a timely process that is prone to human error that can lead to catastrophe failure of the electric system. The process the reduces the likely hood of human error and allows for an expedited reliable response time.

The next steps reduce the likely hood of human error and provides reliability to our customers. They include significant expansion for situational awareness, enhancement of available information, the integration of the DMS / Data-Diode system currently under development for the Protection / Controls group. DMS / Data-Diode is intended to replace the manual operator entry method used at substations. We intend to add a series of regional maps and summary tables to provide more extensive situational awareness of both the transmission, sub-transmission, and area stations. Two new FTE will work at the Energy Control Center with substations and Engineering will work with the DMS Data Diode resource application to installed the necessary equipment (firewalls, modems ,media converters, etc..) spanning all 40 transmission and 63 sub-transmissions substations. To be integrated with TNVS to provide a reliable source of information over the next 4 years. This automated alternative data monitoring system will replace or augment the slow and unwieldy manual data-entry method currently in use. This includes updates the TNVS Server to the latest AVS/OpenViz codebase and contains a full UX update.

Justification Summary:

The Transmission Network Visualization System (TNVS) is a computer application that allows Con Edison users to access near-real-time transmission system information through the company's intranet. This greatly leverages the availability of system situational awareness to a much larger audience of operators and engineers.

For TNVS, there are no alternatives for display graphics showing near real-time information that would be available for Engineering and Management staff that do no have direct access to the Energy Control Center. This information is a major time/work saver under normal operating conditions, and is critical during system events and emergencies, and needs to be available to the widest number of users.

TNVS is the only Energy Management System (EMS) backup system if the Energy Control Center losses the EMS. TNVS is required in order to provide continued safe and reliable operation of the Electric and Steam Systems or our employees and customers. Thus, there are no alternatives for this system as it is a controlled system that if rendered available would lead to a complete loss of Con Edison Electric System and significant damage to the Steam System. The wider roll-out of this application in both scope and availability will enable greater situational awareness to operators and supporting personnel during a potential dark-sky event. The application was recently updated from client-based to browser-based to enable this expansion, along with a prototype of version of TNVS to be used by System Ops personnel upon failure of the SCADA systems at the ECC and AECC.

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
N/A

2. Supplemental Information

Alternatives

This is a stand alone life boat system with no alternatives.

Risk of No Action

Risk 1 – Loss/ damage to the Bulk Electric System and Steam System
Risk 2 – Potential fines from local and federal regulatory entities
Risk 3 – Damage to Con Edison reputation

Non-Financial Benefits

- Increased safety, reliability, customer satisfaction
- Improved workflows and communication among departments
- Stronger relationships with community or with regulators
- Ensuring regulatory compliance

Summary of Financial Benefits and Costs (attach backup)
1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Basis for estimate
N/A

Project Risks and Mitigation Plan
N/A

Technical Evaluation / Analysis

Project Relationships (if applicable)
N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	**Actual 2021**	**Actual 2022**	**Actual 2023**	**Test Year (O&M Only)**	**Forecast 2024**
O&M						
Regulatory Asset						
Capital	378.00	134.00	498.00	447.00		862.00

2025-2029 Request:
Total Request by Year:

	2025	**2026 (RY1)**	**2027 (RY2)**	**2028 (RY3)**	**2029**
O&M					
Regulatory Asset					
Capital (Total)	$1,500.00	$2,500.00	$2,500.00	$2,500.00	$2,500.00
Labor	$320.00	$1,500.00	$1,500.00	$1,500.00	$1,500.00
M&S	$1,000.00	$800.00	$800.00	$800.00	$800.00
Contract Svcs.	$120.00	$125.00	$125.00	$125.00	$125.00
Other					
Overheads	$60.00	$75.00	$75.00	$75.00	$75.00

S&TO
2025-2029

1. Project / Program Summary

Type: ☐ Project ☒ Program	**Category: ☒ Capital ☒ O&M ☐ Regulatory Asset**
Work Plan Category: ☒ Regulatory Mandated ☐ Operationally Required ☐ Strategic	
Project/Program Title: Cyber Security and NERC Compliance	
Project/Program Manager: Frank Santoro	**Project/Program Number (Level 1): 23287750**
Status: ☐ Initiation/Planning ☐ In-Progress (Projects Only) ☒ On-going (Programs Only)	
Estimated Start Date:	**Estimated Date In Service: Ongoing**
2025-2029 Funding Request ($000) **Capital: 29,600.00** **O&M: 3,990.00**	

Work Description:

A dedicated cybersecurity team was formed as part of a re-organization within System Operation in late 2022. Theis group has two objectives which are to maintain and improve the cybersecurity of the Energy Control Center and energy management systems to prevent intrusions, and to ensure bulk power System Operation remains compliant with all applicable North American Electric Reliability Corporation (NERC) standards. Meeting these two objectives requires constant efforts that involve maintaining and upgrading existing technology (software and hardware), implementing new technology, performing third party penetration tests and vulnerability assessments, and conducting internal assessments of controls and policies.

Set forth below is a list of currently proposed projects for calendar year 2026 (*i.e.*, Rate Year 1). However, as systems and technology improve, these projects may be substituted to meet the company's needs.

Implementation of:

- A packet broker solution to better integrate cybersecurity solutions and support future CIP requirements
- Load balancers to help with high availability of security and operational systems and applications
- Patch Management Solution
- Networking port security platforms to better secure what devices can gain access to the network when physically plugged in

Set forth below is a list of currently proposed projects for calendar year 2027 (*i.e.*, Rate Year 2). However, as systems and technology improve, these projects may be substituted to meet the company's needs.

Implementation of

- Cybersecurity Automation solution to help augment response and actions to be taken

- Code Scanning Solution to help determine potential cybersecurity issues with custom written applications within the ECC
- User Endpoint Behavior Analytics (UEBA) to help provide additional insight for the Cybersecurity team
- A deception solution
- Replacing firewalls as the existing Firewalls in use will be end of life

Set forth below is a list of currently proposed projects for calendar year 2028 (*i.e.*, Rate Year 3). However, as systems and technology improve, these projects may be substituted to meet the company's needs

Implementation of

- Firewall configuration management tool
- Other technology as needed
- A refresh of SIEM Hardware

As part of these proposed projects this whitepaper is requesting funding for 10 FTE as broken down below

- 6 FTE will work in rotating shift to staff a single 24x7 cyber-watch position
- 1 FTE will be responsible for managing the cyber-watch team
- 2 FTE will be responsible for building and maintaining cybersecurity tools
- 1 FTE will help expand the networking team and will be responsible for supporting and maintaining the network and firewalls.

Capital labor is requested to maintain the level of current staffing to implement these efforts. O&M Labor is requested to maintain existing systems and the staffing necessary for upkeep.

Justification Summary:

This project is necessary as the cybersecurity of the Energy Control Center and our bulk power system is critical. Cybersecurity requirements for IT systems associated with the company's business operations have continued to grow as the risks and threats of cyber-attacks have increased. If we do not invest in the cybersecurity of our network, the risk of an unwanted intrusion and impacts to our customers, significantly increases. Additionally, the company will be exposed to fines of up to $1.2M per day per violation if we are not able to comply with NERC standards. New technologies and enhanced processes (*e.g.*, automation) are needed to mitigate the new risks from file-less malware, supply chain cybersecurity risks, and continually evolving advanced persistent threats

Relationship to Broader Company Plans, Initiatives and the NYS Climate Leadership and Community Protection Act
N/A

2. Supplemental Information

Alternatives

Alternative 1 description and reason for rejection
Do Nothing

If we were to do nothing and not continue to invest and upkeep our cybersecurity, there would be significant risk exposure for our bulk power system that is used to maintain electricity to our customers and neighboring utilities. The result could mirror what occurred in Ukraine in 2015 where their power grid experienced a cyberattack which resulted in loss of power to customers and millions of dollars in damages to physical equipment such as transformers and feeders. Additionally, this can open the company up to fines if we cannot meet any new standards that are established.

Risk of No Action
With no action there is the risk of exposure to cybersecurity intrusions, impact to delivery of electricity and steam to customers, damage to company equipment, and fines of up to $1.25M per day, per violation to the company for not maintaining compliance with NERC standards

Non-Financial Benefits
This project allows for ensuring regulatory compliance, increased network reliability, resiliency, and efficiency, and Secure and improved energy delivery

Summary of Financial Benefits and Costs (attach backup)
1. Cost-benefit analysis (if required)
N/A

2. Major financial benefits
N/A

3. Basis for estimate

Historic purchases are used, as well as vendor presentations and Internet sources.

Project Risks and Mitigation Plan

Risk 1 Appropriate resources — Mitigation plan – hire employees and contactors to help perform the work

Technical Evaluation / Analysis
Planning and analysis on all technologies introduced will be performed with IT advisors, vendors, and Company stakeholders to ensure the selection of optimal solutions.

Project Relationships (if applicable)

N/A

3. Funding Detail ($000)

Historic Spend

	Actual 2020	Actual 2021	Actual 2022	Actual 2023	Test Year (O&M Only)	Forecast 2024
O&M						
Capital	$1,003.00	$900.00	$1,391.00	$2,653.00		$7,900.00

2025-2029 Request:

Total Request by Year:

	2025	2026 (RY1)	2027 (RY2)	2028 (RY3)	2029
O&M	0.00	891.00	1,033.00	1,033.00	1,033.00
Regulatory Asset					
Capital (Total)	4,800.00	7,200.00	6,200.00	5,700.00	5,700.00
Labor	2,650.00	2,600.00	2,600.00	2,600.00	2,600.00
M&S	1,550.00	4,000.00	3,000.00	2,500.00	2,500.00
Contract Svcs.	600.00	600.00	600.00	600.00	600.00
Other					
Overheads					