Q. Please state your name and business address.
A. My name is Michele M. Campanella and my business address is 4 Irving Place, New York, New York 10003.
Q. By whom are you employed and in what capacity?
A. I am employed by Consolidated Edison Company of New York, Inc. ("Con Edison" or the "Company") as the Director of Security Services.
Q. Please describe your educational background.
A. I graduated from Clarkson University, Potsdam, New York with a Bachelor of Science degree in Accounting in 1978 and from New York Law School, New York, New York, with a Juris Doctor degree in 1989.
Q. Please describe your work experience.
A. I was a Special Agent of the Federal Bureau of Investigation ("FBI") from 1980 to 2008. Among other duties, I served as the Assistant Special Agent in Charge ("ASAC") in the Washington Field Office, a position that included oversight of the Security Branch. As the ASAC, I was responsible for the protection of the Attorney General of the United States and the Director of the FBI, the physical security of the properties within the Washington Field Office territory, and the investigative services related to personnel security, including polygraphs, background

investigations, and clearances. Since September 2008, I have been the Director of Security Services for Con Edison.

Q. Please generally describe your current responsibilities.

A. As the Director of Security Services, I formulate and direct security policies, practices and procedures for the Company. I direct the investigative and security related activities of twenty-two investigators and staff; act as a liaison with Federal, State and local law enforcement agencies; advise senior executives on security-related matters; direct physical security surveys of Company facilities; and make and implement security recommendations throughout the Company. In addition, I develop specifications and monitor the performance of contract guard services and implement training requirements for Company security personnel.

Q. Do you belong to any professional societies or organizations?

A. I am an active member of the Security Committees for both the American Gas Association and the Edison Electric Institute.

Q. What is the purpose of your testimony?

A. My testimony addresses the essential topic of building

upon the Company's existing security programs by providing for the continued maintenance of the equipment at our Security Operations Center ("SOC"), enhancing the capabilities of the SOC, and hiring two additional technical systems specialists.

Q. What is the projected capital cost for the security project?

A. The projected capital cost is $1.427 million.

Q. What are the projected O&M costs associated with the security requests?

A. The projected O&M cost associated with the security requests is $413,000 total for the rate year.

SOC

Q. Explain the genesis of the SOC and what it does for the Company.

A. In August 2002, the New York State Public Service Commission ("PSC") issued an Order directing all New York State utility companies to retain consultants to evaluate the physical security of their systems. The Company hired Safir-Rosetti, an international security consulting firm, to conduct an extensive assessment of Con Edison's critical facilities and operations, its general security protocols and procedures, and its planning and capabilities for emergency/disaster

recovery and business continuity. In their confidential report, issued on January 17, 2007, Safir-Rosetti recommended "All physical security control, including access management systems, CCTV systems and real-time site intrusion detection monitoring, should be conducted from a consolidated, Company-wide Security Control Center. This will provide a central communications and response point for all security events and alarms for all of Con Edison's critical facilities."

Q. Did the Company implement Safir-Rosetti's recommendations?

A. Yes. In 2007, the Company's Corporate Security team designed and oversaw the construction of the SOC. The SOC monitors, controls and manages the security of disparate technologies from one central location on a video wall on a real-time basis. The video wall is a giant screen much like a television. It displays either the activity from one camera or is subdivided in numerous configurations to show activity at over one hundred camera locations.

Q. What exactly is monitored at the SOC?

A. At the SOC, on a 24 hour, seven day per week basis, two contract security guard specialists monitor:

- A card access system consisting of 58 locations;
- 216 control panels and 836 readers (the number of card access locations and cameras installed increases every month);
- A CCTV system comprised of 750 cameras at 57 locations;
- Three hundred zones for intrusion detection; and
- Six locations and 60 zones for burglar alarms, and four locations, at customer service centers, for threats to the tellers.

Q. You stated you need to provide for continued maintenance of the SOC. What does that entail?

A. The first of my requests is for $137,000 per year in O&M for the continued maintenance of the video wall at the SOC through a maintenance services contract. Because the video wall is integral to the integrity of the security at the Company, it is always on and monitored and, therefore, keeping the equipment maintained is vital.

Q. What work would be performed under the maintenance service contract?

A. The maintenance service contract for the SOC would include two visits per year to the SOC for realignment

as well as color balancing of the 12 cubes, and the cleaning of the interior of the cubes. This work also includes a full re-lamping of the video wall once a year (24 lamps-one active and one spare) per cube installed. The maintenance service contract also covers repairs to the display server, application server and rendering servers. The projected price also includes a software upgrade, if needed, as well as technical support by telephone. The Company is currently in the process of negotiating a contract for the maintenance of the video wall.

Q. Do you have an exhibit that provides additional information regarding maintenance contract for the SOC?

A. Yes.

Q. Was this exhibit prepared under your direction and supervision?

A. Yes.

MARK FOR IDENTIFICATION AS EXHIBIT __ (MMC-1)

Q. Please continue.

A. We also plan to enhance the capabilities of the SOC by adding a Geo-Spatial Management and Access Control automation system.

Q. Why do you need this system?

A. As I noted earlier, every month additional access

control panels, cameras, and alarms are connected to the SOC. As more Company sites are interfaced with the SOC, the amount of information increases exponentially. With the increasing amount of data coming into the SOC, the Company relies on the two SOC console operators to first detect and then manually maneuver cameras to focus on any incidents occurring. The need for the two console operators to process these large volumes of information could lead to potential omissions, delayed response times, and possibly, inaccurate input. These potential issues could have significant security ramifications.

Q. How would the Geo-Spatial Management and Access Control automation system address these potential problems?

A. This computer system would automate the access control and intrusion detection alarms. If a door were to be forced open, the new computer program would move the corresponding mapped location to the foreground on the video wall for the console operators to immediately see. The camera at the subject location would automatically focus on the situation and would alert the operator at the SOC. This would provide immediate notification, maximizing the efficiency of the operator by reducing both response time and the necessity for

human data parsing. In addition, it would automatically alert the SOC if a camera failed and provide advanced notification of nuisance type alarm activity to protect against unnecessary outages.

Q. Why was this system not implemented in the original design?

A. This is a new technology not available when we designed and implemented the SOC. Since learning of the system, we have researched various prototypes to determine if the product we selected could be integrated to fit our needs.

Q. What are the requirements of this system?

A. This is a software system that will require integration into the three existing security systems of the Company: the MSSQL card access; Activu; and the Keltron Alarm systems. There are no software systems that will interface with our current systems without considerable modification. We have determined this to be the most cost-efficient solution to meet our needs.

Q. What are the costs associated with installing and implementing this system?

A. The system and related costs are expected to cost approximately $1.427 million, including $1.4 million for the system; Information Resource labor for network

wiring of $2,000; and the use of a contractor to assist in the integration of the system estimated at $25,000. The system would be installed in the rate year.

Q. Are there maintenance costs associated with this system?

A. The maintenance costs the first rate year would be included in the contract price as part of the warranty. Thereafter, the annual maintenance cost of the Geo-Spatial Management and Card Access Automation System would be $120,000.

Q. Do you have any exhibits that provide additional information regarding this system and the related expenses?

A. Yes, I have two exhibits.

Q. Were these exhibits prepared under your direction and supervision?

A. Yes.

MARK FOR IDENTIFICATION AS EXHIBITS ___(MMC-2, MMC-3)

EMPLOYEE SUPPORT

Q. Does the Company require any additional employees for the security department?

A. Yes. The Company requires two additional employees at an estimated annual cost of $179,000. The rate request reflects $156,000 based upon anticipated hire months of

April and August 2010.

Q. Please explain how the mission of corporate security has evolved in recent years.

A. Corporate Security's mission has evolved and grown since September 11, 2001. Almost all of this growth has focused on technical aspects of security, which includes evaluating, analyzing, recommending and installing effective electronic security systems to better protect our critical infrastructure.

Q. Please explain the need for the two additional personnel.

A. The two employees are required to maintain a reliable and secure workplace for our employees and contractors. They are also required for the enhanced security of our customers at our customer service centers. The Company has an operational need for two highly specialized Systems Specialists proficient in internal and external electronic security protection systems not just for connecting new systems to the SOC, but for a myriad of security-related technical projects.

Q. Can you please expand on that?

A. Yes. The Company determined, through a review of prior construction projects, it was more cost-efficient to include security measures in the design of a new or

upgrade of a facility as opposed to adding those measures after the construction. In December 2008, a Corporate Instruction was approved which mandates Corporate Security to evaluate security drawings and specifications for new facilities or facilities which will be upgraded, prior to the Company submitting these to bidders. This technical review also includes software setup, programmed matrices for CCTV systems and associated networking for the security associated with each facility. The involvement by security specialists from my department also includes review of submitted bids to ensure the technical merits have been addressed. This provides subject matter expertise to enhance risk aversion and avoid cost overruns. The two additional technical security specialists would also be utilized to conduct critical site assessments with members of the PSC. In January 2009, the Company added three more sites to our list of critical sites for a total of 40 critical sites. At present time, 23 of the Company's critical sites have some component of their security connected to the SOC. As time permits, the additional manpower would be utilized to integrate more of these critical sites to the SOC.

Q. Are there any other functions additional specialists

would address?

A. Yes. Additional personnel would enable Corporate Security to expand the scope of work we currently do to include: corrective and preventative maintenance; test technical security systems; determine optimal equipment logistics and inventory; and bench repair of defective technical security system to the component level. These additional tasks would prove to be cost effective methods to extend the life of the equipment and ensure the reliability of the system.

Q. Do you have an exhibit that provides additional information regarding the hiring of the two specialists?

A. Yes.

Q. Was this exhibit prepared under your direction and supervision?

A. Yes.

MARK FOR IDENTIFICATION AS EXHIBIT __(MMC-4)

Q. Does this complete your testimony?

A. Yes, it does.

2010 O&M – Security Services

Project/Program Title	Maintenance Agreements – Security Operations Center (SOC)
Status	In Service
Estimated Service Date	January, 2010
Work Plan Category	Regulatory

Work Description: Maintenance agreements for video wall and components to insure 24/7 operability which currently was under installation guarantee. To assure continued maintenance of equipment propose entering into a two-year service contract at $137 K per year.

Justification: Annual maintenance agreement to service equipment contained in the SOC. Scheduled preventive maintenance included in contract based on the specific needs of the equipment. PM includes adjustments, cleaning, lubrication, replacement of defective parts, and retrofitting for engineering changes.

- Alternatives: pay as needed basis for service calls which would prove costly compared to agreement that would cover all parts.
- Risk of No Action: SOC equipment would fail taking Center off-line

Summary of Financial Benefits and Costs: The cost of pay you go estimated to cost more and not provide for reliable repairs.

- Non-financial Benefits : The running of the SOC provides an important security measure to protect the critical infrastructure of the Company.
- Technical Evaluation/Analysis:
- Sensitivity Analysis :
- Project Relationships : The construction of SOC and related equipment requires continuous maintenance agreements.

Estimated Completion Date: 2010

Status: **Plan to put service contract into place.**

Funding ($000):

Approved 2009	Forecast RYE 2011	Forecast RYE 2012	Forecast RYE 2013	Forecast Total 2011-2013
-	137	137	137	411

2010 O&M – Security Services

Project/Program Title	Security Operations Geo- Spatial Camera maintenance Contract
Status	Planning
Estimated Service Date	March 2011
Work Plan Category	Regulatory

Work Description: Maintenance agreement for Geo-Spatial Camera and Access Control Automation to insure 24/7 operability for Capital request of $1.427 M in 2010: Starting in 2011 would incur as follows:

Units per Year: cost per year – annual contract - $120,000
Mandatory: continuing service agreement per specification
High-level schedule: renewable 3 year contracts

Justification: Annual maintenance agreement to service equipment contained in the SOC. Scheduled preventive maintenance included in contract based on the specific needs of the equipment. PM includes adjustments, cleaning, lubrication, replacement of defective parts, and retrofitting for engineering changes.

- Alternatives: pay as needed basis for service calls which would prove costly compared to agreement that would cover all parts.
- Risk of No Action: SOC Geo-Spatial equipment would fail taking camera off-line
- Summary of Financial Benefits and Costs:
- Non-financial Benefits : The running of the SOC provides an important security measure to protect the critical infrastructure of the Company. The maintenance contract is required to assure continued use of system.
- Technical Evaluation/Analysis:
- Project Relationships : The construction of SOC and related equipment requires continuous maintenance agreements.

Estimated Completion Date: After Capital installation in 2010 would be annual maintenance cost.

Status: Planning for maintenance after installation.

Funding ($000):

Forecast 2010	Forecast RYE 2011	Forecast RYE 2012	Forecast RYE 2013	Forecast Total 2011-2013
-	120	120	120	360

2010 Capital – Security Services

Project/Program Title	Security Operations Geo-Spatial Camera and Access Control Automation
Status	Planning
Estimated Service Date	March 31, 2011
Work Plan Category	Regulatory

Work Description:

During January, 2008 the Security Operations Center was opened providing an all inclusive security monitoring system. The Center has enhanced our ability to provide maximum protection of our facilities.

Introduction of Geo-Spatial management

Geospatial mapping provides the user with an interface which will provide a geographical display illustrating:

- Illustrating the exact location via aerial picture
- Insertion of icons which represent camera locations, type, and field of view capability
- Icon representation of Access Control Doors
- Icon representation of Intrusion detection zones

A high resolution aerial photo or floor plan would be inserted in to the system. This would provide the foreground for the map of cameras and other infrastructure. This picture would not be static. The operator would be able to click on any of the active icons (cameras, doors etc.) and automatically pull up the device and take control or monitor.

This system would also automate the access control and intrusion detection alarms. If a door were to be forced open or chucked open, the corresponding mapped location would move to the foreground on the operators desktop. The icon associated with exact door where the intrusion occurred would changed color and the associated camera would automatically open in a window on either or both the operators computer monitor or a portion of the large display wall which would be utilized to display alarm events only. This would provide immediate notification; maximize the efficiency by reducing both response time and the necessity for human data parsing.

There are several other aspects that greatly improve the ability to automate response and improve the reliability of the system such as:

- Automatic camera failure detection
- Advanced notification of possible nuisance type alarm activity thru trend analysis.

Both of these aspects provide information necessary to manage this tremendous amount of equipment and protect the investment against unnecessary outages.

This system will tie into one interface. It will need to be transparent to the user. It will require integration into the MSSQL card access back end, Activu (the display solution in place at the SOC) and the Keltron Alarm interface. It will require vast amounts of programming and designing. There currently is no such system that is an off the shelf product, which can be implemented without heavy modification.

2010 Capital – Security Services

Additional installation costs require Information Resource labor for network wiring working approximately 4o hrs. Estimated labor cost is $2,000.00. The use of a contractor to assist in the integration of the system is estimated at $25,000.00.

Justification:

The Con Edison Security Infrastructure currently in place is a complex myriad of several types of systems. These systems were implemented as a result of Corporate Security's risk assessments. These findings were then challenged by an outside consultant who performed their own assessments. The consultant's findings were consistent with Corporate Security's and the recommendations were thus implemented. These systems include:

- Card Access – 58 Locations, 171 Control Panels , 766 Readers (Doors)
- CCTV - ~750 cameras, 57 Locations (This number increases with ongoing projects)
- Intrusion detection – ~300 Zones
- Burglar – 6 Locations, 60 Zones
- Duress - 4

These systems which had been implemented over the past decade were originally monitored locally onsite or in the case of Burglar and Duress, by a monitoring service which charged a monthly monitoring fee.

When an event occurred the information necessary to provide real time analysis, and aid in first response was unavailable unless you physically went to the location where the incident was occurring. This was because remote access and monitoring of these devices in a central location was not available at that time.

In 2007 the Con Edison Corporate Security Technical Team designed and constructed the Security Operations Center. This genesis became the Mission Critical Location which currently provides Con Edison Corporate Security the ability to monitor, control, and manages all of the distributed technologies from one centralized location. For the first time ever we are now able to utilize the multi-layer, deter, delay, detect and respond philosophy associated with the design intent of the implemented Security Infrastructure.

With the current technology in place we have the ability to receive real time events that are generated from these systems. This was a crucial step in the overall design topology necessary to advance and increase the efficiency related to incident mitigation. This does not go without some inherent caveats, primarily, extended response time of the operator due to the large amount of data that needs to be parsed by human intervention. There is an apparent necessity to automate how some of these independent systems operate.

For Example:

Card Access can provide us with the information that a door may have been forced open. It will tell us when and where the event occurred. Verification of the data in order to provide the correct response action can be further enhanced by being able to view the exact are of the location with one of the CCTV cameras. The primary problem with this is at any given location there may be many

2010 Capital – Security Services

cameras. The success rate can vary because the operator is not familiar with any of the locations. The operator at the SOC would have to one by one call up each camera manually in order to try to locate the incident. The operator still will not know what the cameras capable field of view is. The camera may be pointing in one direction however it may be capable of being remotely controlled and pointed at the area of the incident.

- Alternatives: Continue with current interaction, involving two console operators who are working 24 hours - 7 days a week. It requires extensive input and possible error. Provide hard copies of maps, which will delay response and require extensive and possibly inaccurate input from the two 24/7 operators in place.

- Risk of No Action: There will be a zero increase in efficiency, probable increase in error rate and increase in cost of management as the infrastructure grows.

- Non-financial Benefits: The system will reduce risk and increase the opportunities to become an investigative tool used to aid in forensic information gathering. Features of the proposed system will provide us the ability to anticipate security infrastructure outages (CCTV, DVR, Access Control and Intrusion Detection) in a timely fashion improving the quality of service and should mitigate increase maintenance costs. .

- Technical Evaluation/Analysis: The purpose of this system is to aid in the mitigation of incident response errors due to system size and complexity.

- Project Relationships : As part of this project any personnel responsible for implementing the design solution will be required to work with the Security Operations Center design contractor

Estimated Completion Date: March 31, 2011

Funding

Approved 2009	Request 2010	Request 2011	Request 2012	Request 2013	Request/Approved 2009-2013 Total
	$1,427				$1,427

2010 O&M – Security Services

Project/Program Title	Corporate Security - Additional Human Resources
Status	Planning
Estimated Service Date	March 2010
Work Plan Category	Demand Growth

Work Description:

Corporate Security has an operational necessity to add two highly specialized Systems Specialists (2H) proficient in internal and external electronic security protection systems.

Justification:

Corporate Security's mission has evolved since September 11, 2001. The increase in manpower has not kept pace with the increase in risk. Almost all of the growth has originated on the technical side of the business and focuses on evaluating, analyzing, recommending and installing effective electronic security systems to better protect our critical infrastructure and integrate these systems to our Security Operations Center (SOC). The addition of two Systems Specialists will be a Program Change for the Technical Section of Corporate Security.

The organizational structure of Corporate Security is composed of three departments. One of these departments handles all the technical aspects of security. This department is comprised of a manager, two Senior Specialists, and four Systems Specialists. Two of the Systems Specialists handle the day to day operations, including the Information Resources (IR) aspects, of the SOC. One of the Senior Specialists is responsible for the access control within CECONY. The remaining personnel: a Senior Specialist, two System Specialists and the Department Manager are responsible for evaluating, reviewing, proposing and, in limited instances, installing technical security equipment to safeguard personnel and prevent unauthorized access to Company equipment, systems, material and information. In addition they oversee security technical equipment which includes access control systems, alarm systems, recorded CCTV systems, motion detectors, intrusion detection systems, etc.

In addition the technical group conducts site assessments with members of the PSC to address all regulatory, federal, state and homeland security requirements. Each year Corporate Security, accompanied by the PSC, documents their evaluation, review and recommendations for the continued security of these critical sites. To fulfill this goal additional Systems Specialists are necessary.

In December 2008, changes to Corporate Policy 860-1, Security Services Responsibilities, mandate "All Company organizations MUST confer with and obtain the approval of Corporate Security prior to commencement of any anticipated procurement of a security related enhancement or new construction project." This entails designing and engineering state of the art security systems relating to new construction and physical security of company properties, providing security drawings detailing all equipment to be installed, assisting Engineering and IR in developing the seamless integration of all security related equipment into the Con Edison "Corporate Network," and developing and maintaining corporate wide security engineering

specification to be utilized by Purchasing, Engineering, IR and Facilities Management for bid purposes.

Risk of no action:

1) Construction projects could be delayed pending Security Systems Specialist review.

2) Some site survey work is currently conducted by non technical security specialists. This is minimally acceptable in addressing physical perimeter's addressed by those technologies that have more visible, tactile characteristics such as guards, fences, gates, and other assets used to prevent entry by unauthorized personnel. But at the critical sites there is a need for expertise in additional technology such as video cameras, access cards, and motion detection equipment.

3) Costs will continue to rise for the maintenance and labor on technical equipment some of which could be mitigated by either early diagnosis of problem or minor repairs made on the site by the Security Specialists.

4) The risk of exposure to theft and sabotage can be mitigated by increased use of technology.

Non-Financial Benefits:

A new area of responsibility (see Corporate Instruction 860-1 supra) includes evaluating security drawings and specifications for the Company including all technical interfaces and system design for submission to contractors and field commissioning (technical direction to site technicians) including software setup (Life Safety and Security), programmed matrices for CCTV systems and associated networking. This involvement by Security is an added layer of oversight and provides subject matter expertise to enhance risk aversion that will be available 24/7 for response to adverse situations.

Additional three sites added to critical infrastructure list for Con Edison of New York. This will entail detailed site assessments to be conducted by the Systems Specialists in conjunction with members of the PSC.

Expand the Scope of Work:

1) Responsibilities will be added to include corrective and preventative maintenance, and testing of technical security systems; equipment logistics and inventory; and bench repair of defective technical security system to the component level. It is anticipated the additional two Security System Specialists would be able to save user organizations critical down time of equipment and mitigate some of the expenses currently paid to contractors for minor repairs.

2) Continue to interface critical sites to the SOC. Currently 23 of the 40 critical sites have aspects that are monitored at the SOC.

2010 O&M – Security Services

3) Add additional alarm systems (fire and burglar) to be monitored by the SOC, which could provide financial benefits to the user organizations by providing higher level of monitoring.

The two recommended System Specialists will provide the experience and capabilities to handle the additional workload and governmental regulatory compliance requirements to better protect the energy infrastructure. We cannot hire a Contractor for this work as our list of Critical Sites and our potential vulnerabilities is vital information we need to protect.

Estimated Completion Date:

Hire first Systems Specialist in April 2010 and the second in June 2010.

Status:

Planning

Funding (000):

Actual 2004	Actual 2005	Actual 2006	Actual 2007	Actual 2008
-	-	-	-	-

Approved 2009	Forecast RYE 2011	Forecast RYE 2012	Forecast RYE 2013	Forecast/Approved Total 2009-2013
-	156	179	179	$514