RIVERSIDE PUBLIC UTILITIES PHYSICAL SECURITY PLAN

PUBLIC REPORT ON RIVERSIDE PUBLIC UTILITIES PHYSICAL SECURITY PLAN FOR DISTRIBUTION-LEVEL FACILITIES

August 9th, 2021

Contents of this document have been redacted for review in public forum

WATER | ENERGY | LIFE

CITY OF RIVERSIDE PUBLIC UTILITIES

TABLE OF CONTENTS

I. OVERVIEW

A. GOAL OF POWER UTILITY SECURITY PLAN

Ensuring the safety of its facilities is a top priority for Riverside Public Utilities (RPU), and RPU prioritizes safety in all aspects of its design, operation, and maintenance practices. The overarching goal of this Power Utility Security Plan is to describe RPU's risk management approach toward distribution system physical security, with appropriate consideration of resiliency, impact, and cost.

RPU recognizes the importance of securing the safety and reliability of its electric system and RPU offers the following in response to CPUC Decision 19-01-018 for "Covered Distribution Facilities".

B. DESCRIPTION OF RIVERSIDE PUBLIC UTILIES

Established in 1895, Riverside Public Utilities (RPU) provides high quality, reliable services to over 81 square miles to 109,000 metered electric customers and almost 65,000 metered water customers throughout Riverside. A dedicated staff of almost 600 people operate, maintain, and support a complex electric and water infrastructure that is worth more than $3.2 billion dollars1. RPU owns 13,912 distribution transformers, 16 substations, more than 1,300 circuit miles of distribution cables connecting them with more than 22,000 poles overhead and more systems underground. The transmission system has almost 100 miles of cable. The 16 substations that serve each neighborhood in the city, have a total of 65 transformers and 54 switchgears.

C. RESULTS OF POWER UTILITY SECURITY PLAN ASSESSMENT

Riverside Public Utilities gathered the requisite information to determine which of its 16 substations meet one or more of the CPUC's criteria for a "Covered Distribution Facilities" as defined in the CPUC Decision 19-01-018. Of the 16 facilities, only 4 substations met one or more of the CPUC's identification criteria. Out of these 4 substations, after conducting a Risk Assessment on each one of them, it was determined that each one should implement a Mitigation Plan, as detailed in sections V and VI of this Physical Security Plan.

This physical security plan has been reviewed by a qualified third party, and RPU has incorporated their comments as applicable.

[1] Popular Annual Financial Report Page 6 Capital Assets available at:
https://riversideca.gov/finance/PDF/Annual%20Financial%20Reports/2020%20PAFR.pdf

II. BACKGROUND

On April 16, 2013, one or more individuals attacked equipment located within Pacific Gas and Electric Company's (PG&E) Metcalf Transmission Substation, ultimately damaging 17 transformers. These individuals also cut nearby fiber-optic telecommunication cables owned by AT&T. In response to the attack, the Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to develop new physical security requirements, resulting in the creation of CIP-014.

At the state level, Senator Jerry Hill authored SB 699 (2014), directing the CPUC to "consider adopting rules to address the physical security risks to the distribution systems of electrical corporations." In response to SB 699, the CPUC's Safety and Enforcement Division, Risk Assessment and Safety Advisory Section (RASA) prepared a white paper proposing a new requirement for investor-owned utilities (IOUs) and publicly owned utilities (POUs) to develop security plans that would identify security risks to their distribution and transmission systems and propose methods to mitigate those risks. The CPUC hosted a series of workshops to better understand the state of utility physical security protections and to seek input on refining their proposal.

To support a statewide improvement of how utilities address distribution level physical security risks, the California Municipal Utilities Association (CMUA), which is the statewide trade association for POUs, coordinated with the state's IOUs to develop a comprehensive Straw Proposal [2] (Joint IOU/POU Straw Proposal) for a process to identify at-risk facilities and, if necessary, develop physical security mitigation plans. The Joint POU/IOU Straw Proposal set out a process for the following: (1) identifying if the utility has any high priority distribution facilities; (2) evaluating the potential risks to those high priority distribution facilities; (3) for the distribution facilities where the identified risks are not effectively mitigated through existing resilience/security measures, developing a mitigation plan; (4) obtaining third party reviews of the mitigation plans; (5) adopting a document retention policy; (6) ensuring a review process established by RPU's governing board; and (7) implementing information sharing protocols.

RASA filed a response [3] to the Joint IOU/POU Straw Proposal that recommended various modifications and clarifications, including a six-step process. Additionally, RASA recommended that the utility mitigation plans include: (1) an assessment of supply chain vulnerabilities; (2) training programs for law enforcement and utility staff to improve communication during physical security events; and (3) an assessment of any nearby communication utility infrastructure that supports priority distribution substations.

---

2 Straw Proposal available at:
https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/R1506009-Updated%20Joint%20Straw%20Proposal%20and%20Cover%20083117%20Filing.pdf.

3 RASA Response available at:
https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/Final%20Staff%20Recommendation%20for%20Commission%20Consideration%20010318.pdf.

In early 2019, the CPUC approved Decision (D.) 19-01-018, which adopted the Joint IOU/POU Straw Proposal as modified by the RASA proposal, with additional clarifications and guidance. D.19-01-018 clarified that where there is a conflict between the Straw Proposal and the RASA proposal, then it is the rule in the RASA proposal that controls.4

D.19-01-018 asserted that the POUs should utilize the Utility Security Plan process described therein. RPU is following the process and issuing this report at this time to reflect its existing commitment to safety and to protecting its ratepayers' investment by taking reasonable and cost-effective measures in an effort to safeguard key assets of its distribution system.

III. PLAN DEVELOPMENT PROCESS

A. PHYSICAL SECURITY PRINCIPLES

The Joint IOU/POU Straw Proposal seeks to support the creation of a risk management approach toward power distribution system physical security, with appropriate considerations of resiliency, impact, and cost. In order to accomplish this risk-based approach, the Joint IOU/POU Straw Proposal identifies several principles to guide the development of each individual utility's program. These principles are the following:

1. Distribution systems are not subject to the same physical security risks and associated consequences, including threats of physical attack by terrorists, as the transmission system.

2. Distribution utilities will not be able to eliminate the risk of a physical attack occurring, but certain actions can be taken to reduce the risk or consequences, or both, of a significant attack.

3. A one-size-fits-all standard or rule will not work. Distribution utilities should have the flexibility to address physical security risks in a manner that works best for their systems and unique situations, consistent with a risk management approach.

4. Protecting the distribution system should consider both physical security protection and operational resiliency or redundancy.

5. The focus should not be on all Distribution Facilities, but only those that risk dictates would require additional measures.

6. Planning and coordination with the appropriate federal and state regulatory and law enforcement authorities will help prepare for attacks on the electrical distribution system and thereby help reduce or mitigate the potential consequences of such attacks.

4 D.19-01-018 at 43, footnote 58 ("Should there be any question of which shall predominate should there be any incongruity or conflict between a utility or SED RASA recommended rule, the SED RASA rule shall apply.").

B. POWER UTILITY SECURITY PLAN DEVELOPMENT PROCESS

RPU utilized a multi-step process to develop this Power Utility Security Plan that is consistent with the Joint IOU/POU Straw Proposal and D.19-01-018. The relevant six steps of that process are the following:

STEP 1: ASSESSMENT/PLAN DEVELOPMENT

RPU staff and consultants prepared a Draft Power Utility Security Plan through the process set forth in Steps 1A, 1B, and 1C.

STEP 1A: IDENTIFY COVERED DISTRIBUTION FACILITIES

RPU evaluated all distribution-level facilities in its service territory that are subject to its control to determine if any facility meets D.19-01-018's definition of a "Covered Distribution Facility" using the seven factors identified in the Joint IOU/POU Straw Proposal.

STEP 1B: PERFORM RISK ASSESSMENT

For every individual Covered Distribution Facility identified pursuant to Step 1A, RPU performed an evaluation of the potential risks associated with a successful physical attack on that Covered Distribution Facility, and whether existing grid resiliency, back-up generation, and/or physical security measures appropriately mitigate identified risks.

STEP 1C: DEVELOP MITIGATION PLAN

If there are any individual Covered Distribution Facilities where the Risk Assessment performed pursuant to Step 1B finds that the existing mitigation and/or resiliency measures do not effectively mitigate the identified risks, then RPU will develop a Mitigation Plan for that Covered Distribution Facility. The Mitigation Plan will use a risk-based approach to select reasonable and cost-effective measures that can either be security focused (*e.g.*, walls or alarms) or resiliency focused (*e.g.*, adequate spare parts).

STEP 2: INDEPENDENT REVIEW

For every Power Utility Security Plan cycle, RPU will document the results of the identification process, risk assessment, and Mitigation Plan development performed pursuant to Steps 1A, 1B, and 1C. This documentation in combination with narrative description in Section IX below, constitutes RPU's Draft Power Utility Security Plan. Each Draft Power Utility Security Plan is submitted to a Qualified Third Party for Independent

Review. The Qualified Third-Party Reviewer will then issue an evaluation that identifies any potential deficiencies in the Draft Power Utility Security Plan as well as recommendations for improvements. RPU will then modify its plan to address any identified deficiencies or recommendations or will document the reasons why any recommendations were not adopted. The combination of the Draft Power Utility Security Plan, the non-confidential conclusions of the Qualified Third-Party Reviewer, and RPU's responses to the Qualified Third-Party Review will constitute RPU's Utility Security Plan.

STEP 3: VALIDATION

RPU will submit its Power Utility Security Plan to a qualified authority for review. Such entity will provide additional feedback and evaluation of RPU's Power Utility Security Plan and, to the extent that this entity is authorized, such entity deems the Power Utility Security Plan as adequate.

STEP 4: ADOPTION

RPU's Power Utility Security Plan will be presented to the City of Riverside's Board of Public Utilities and Riverside City Council for approval.

STEP 5: MAINTENANCE

RPU will refine and update the Power Utility Security Plan as appropriate and as necessary to preserve plan integrity.

STEP 6: REPEAT PROCESS

RPU will repeat this six-step process at least once every five years.

IV. IDENTIFICATION OF COVERED DISTRIBUTION FACILIITES (STEP 1A)

As described in Section III, Step 1A of the Utility Security Plan process involves assessing all distribution-level facilities that are subject to the control of RPU to determine which facilities are "Covered Distribution Facilities" subject to the need for a risk assessment. This Section describes the factors that RPU used to evaluate its distribution facilities and the results of its evaluation.

A. IDENTIFICATION FACTORS

The Joint IOU/POU Straw Proposal defines seven screening factors to determine if a facility is a "Covered Distribution Facility." Some factors require additional definitions and/or clarifications in order to be applied to RPU's facilities. Table 1 provides the Joint IOU/POU Straw Proposal's Identification Factors as modified/clarified by CMUA and adopted by RPU.

Table 1: Joint IOU/POU Straw Proposal's Identification Factors. Adopted by RPU

No.	Joint IOU/POU Straw Proposal Description	Additional Clarification
1	Distribution Facility necessary for crank path, black start, or capability essential to the restoration of regional electricity service that are not subject to the California Independent System Operator's (CAISO) operational control and/or subject to North American Electric Reliability Corporation (NERC) Reliability Standard CIP-014-2 or its successors	No additional clarification.
2	Distribution Facility that is the primary source of electrical service to a military installation essential to national security and/or emergency response services (may include certain airfields, command centers, weapons stations, emergency supply depots)	No additional clarification.
3	Distribution Facility that serves installations necessary for the provision of regional drinking water supplies and wastewater services (may include certain aqueducts, well fields, groundwater pumps, and treatment plants)	An installation provides "regional drinking water supplies and wastewater services" if it is the primary source of drinking water supply or wastewater services for over 40,000 customer accounts for an area with a population of over 100,000.
4	Distribution Facility that serves a regional public safety establishment (may include County Emergency Operations Centers; county sheriff's department and major city police department headquarters; major state and county fire service headquarters; county jails and state and federal prisons; and 911 dispatch centers)	RPU defines "regional public safety establishment" as any of the following: (1) Headquarters of a major police or fire department serving 1.5 million population with at least 1,000 sworn officers; (2) County Sheriff's Department Headquarters; (3) County Emergency

		Operations Center; (4) County/State Fire headquarters; (5) a California State Prison; (5) a United States Penitentiary; or (6) a Federal Correctional Institute.
5	Distribution Facility that serves a major transportation facility (may include International Airport, Mega Seaport, other air traffic control center, and international border crossing)	In addition to the facilities listed in the Joint IOU/POU Straw Proposal, RPU defines a "major transportation facility" as any transportation facility that has (1) an average of 600 or more flights per day; or (2) over 50,000 passengers arriving or departing per day.
6	Distribution Facility that serves as a Level 1 Trauma Center as designated by the Office of Statewide Health Planning and Development	No additional clarification.
7	Distribution Facility that serves over 60,000 meters	No additional clarification.

B. IDENTIFICATION ANALYSIS

In performing this identification analysis, RPU is assessing all distribution level facilities that are subject to its exclusive control, or if the facility is jointly owned, the joint ownership agreement identifies RPU as the entity responsible for operation and maintenance. The specific types of facilities include all RPU's distributing substations, as well as [redacted]

Based on this scope, RPU has identified all these 16 substations that are subject to this identification analysis. Of these 16 substations, four substations fall within one of the categories listed above. Table 2[5] summarizes the results of RPU's identification analysis for the "Covered Distribution Facilities". Facilities that meet the criteria for any category are indicated by an 'X'.

Table 2: Results for Identification of Covered Distribution Facilities

Facility ID	1. Crank Path, Black Start	2. Military Installation	3. Regional Drinking Water/ Wastewater Services	4. Regional Public Safety	5. Major Transportation Facility	6. Level 1 Trauma Center	7. Over 60,000 Meters
Facility 1 – Redacted			X				
Facility 2 – Redacted			X				
Facility 3 – Redacted				X		X	

[5] Due to security reasons, names of the facilities have been removed.

Facility 4 – Redacted	X						
Facility 5 – Redacted							
Facility 6 - Redacted							
Facility 7 – Redacted							
Facility 8 – Redacted							
Facility 9 – Redacted							
Facility 10 - Redacted							
Facility 11 – Redacted							
Facility 12 – Orangecrest							
Facility 13 – Redacted							
Facility 14 – Redacted							
Facility 15 – Redacted							
Facility 16 - Redacted							

V. RISK ASSESSMENT (STEP 1B)

A. METHODOLOGY

Pursuant to the process identified in the Joint IOU/POU Straw Proposal and D.19-01-018, RPU assessed the potential risks associated with a successful physical attack on each of the Covered Distribution Facilities identified in Section IV above. For purpose of this analysis, a physical attack is limited to the following: (1) theft; (2) vandalism/sabotage; and (3) discharge of a firearm. A "successful physical attack" is limited to circumstances where a theft, vandalism/sabotage, and/or the discharge of a firearm has directly led to the failure of any elements of the Covered Distribution Facility that are necessary to provide uninterrupted service to the specific load identified in Section IV.

In order to perform this risk analysis, RPU evaluates the relative risk that (1) a physical attack on a Covered Distribution Facility will be successful considering the protective measures in place; or (2) that the impacts of a successful attack will be mitigated due to resiliency and other measures in place.

B. MITIGATION MEASURES STUDIED

D.19-01-018 identifies the specific mitigation measures that a utility should consider when performing this risk analysis.

Table 3 lists these mitigation measures and provides additional clarifications that are adopted by RPU from CMUA that are necessary to apply these measures to the RPU's territory.

Table 3: Description of Mitigation Measures Studied

Measure	D.19-01-018 Description	Additional Clarification
1	The existing system resiliency and/or redundancy solutions. (e.g., switching the load to another substation or circuit capable of serving the load, temporary circuit ties, mobile generation and/or storage solutions).	No additional clarification.
2	The availability of spare assets to restore a particular load.	No additional clarification.
3	The existing physical security protections to reasonably address the risk.	No additional clarification.
4	The potential for emergency responders to identify and respond to an attack in a timely manner.	Each facility is evaluated based on the likelihood that a law enforcement officer would generally be able to arrive at the Covered Distribution Facility within 15 minutes of a report from the public of a break-in or attack, or of RPU notifying the law enforcement agency of triggering of an alarm at the facility.

5	Location and physical surroundings, including proximity to gas pipelines and geographical challenges, and impacts of weather.	RPU evaluated this element based on the proximity of the Covered Distribution Facility to populated areas and the extent to which the interior of the facility is shielded from view and access due to walls, vegetation, or other physical obstructions.
6	History of criminal activity at the Distribution Facility and in the area.	RPU evaluated the property crime rates in the immediate vicinity of the Covered Distribution Facility and compared those crimes rates to property crime rates for the county and the state to determine if the area is subject to a higher-than-average incidence of property related crimes.
7	The availability of other sources of energy to serve the load (e.g., customer owned back-up generation or storage solutions).	No additional clarification.
8	The availability of alternative ways to meet the health, safety, or security.	No additional clarification.
9	Requirements served by the load (e.g., back up command center or water storage facility).	No additional clarification.

C. RISK ASSESSMENT

Based on the process described in the Joint IOU/POU Straw Proposal and the direction provided in D.19-01-018, RPU has determined that of the four (4) Covered Distribution Facilities identified in Section IV, the existing programs and measures effectively mitigate the risks of a physical attack for all the Covered Distribution Facilities.

A risk evaluation was conducted, using existing conditions and mitigation measures present at each substation, to ascertain the risk level for each facility.

To this end, a Conditional Assessment of the existing substation conditions was conducted at each facility, including electrical system conditions, physical security conditions, crime rates of the particular areas, as well as history of crime at the substations.

The result of this conditional assessment shows that all four covered facilities feature high resiliency even under the loss of a single element due to its redundant electrical configuration, as well as strongly secured facilities due to physical protection measures. The electrical system has been built to continue operating successfully at rated capacity even under the loss of a single element, i.e., N-1 contingency scenario. The distribution system is fully redundant with back up feeds for the loss of any circuit of the system. There is also an on-going conversion from ceramic insulator to polymer insulator. Finally, the SCADA system is being upgraded to include a Distribution Automation system to remotely operate distribution

switches to expedite power restoration. Appendix A of this report provides a more detail description of the survey conducted for this Conditional Assessment of the covered facilities.

A detailed Risk Analysis was conducted at each of the four covered substations. Details of this analysis can be found in Appendix B of this report. The analysis concludes that the level of risk for any threat of attack (theft, vandalism/sabotage, or firearm discharge) at any of the four facilities is either Low or Mid. This is mainly due to the strong physical security measures in place. However, if an attack were to defeat the security measures in place, the strong resiliency and redundant characteristic of the electrical system will minimize the impact of the attack in terms of outage time to critical loads. These features of all four covered substations makes any probability and/or impact of a successful attack relatively low. However, there are areas where improvements could further enhance the physical security at these substations. Mitigating measures have been recommended for these cases.

The tables 4 through 7 below summarizes the results of the Risk Assessment conducted at each of the covered facilities and presents the risk level at each of the areas where vulnerability of a physical attack to the facility has been analyzed.

Table 4: Risk Index Results for Redacted

		[redacted] SUBSTATION	SUCCESSFUL PHYSICAL ATTACK Risk Index
1	The existing system resiliency and/or redundancy solutions (e.g., switching the load to another substation or circuit capable of serving the load, temporary circuit ties, mobile generation and/or storage solutions)	**1. Grid Resiliency**	**LOW**
		1.1 Capability of Switching the load to another substation	LOW
		1.2 Circuit Ties Capable of Serving the load	LOW
		1.3 Mobile Transformer	LOW
2	The availability of spare assets to restore a particular load.	**2. Spare Assets**	**LOW**
		2.1 Minimum Critical Spare Parts Stock on site	LOW
		2.2 Spare Parts Stock in a warehouse	LOW
3	The existing physical security protections to reasonably address the risk.	**3. Existing Physical Security**	**LOW**
		3.1 Concrete block masonry walls/Chain Link Fence	LOW
		3.2 Security Cameras	LOW
		3.3 Lighting	LOW
		3.4 Motion Detection	LOW
		3.5 Access Control	LOW
4	The potential for emergency responders to identify and respond to an attack in a timely manner.	**4. Emergency Responders**	**LOW**
		4.1 Local Police Agreement for Emergencies	MID
		4.2 Distance from police/fire dept. and time to respond	LOW
5	Location and physical surroundings, including proximity to gas pipelines and geographical challenges, and impacts of weather.	**5. Location**	**LOW**
		5.1 Geographical Challenges	LOW
		5.2 Impacts of Weather Events	LOW
6	History of criminal activity at the Distribution Facility and in the area.	**6. Criminal History**	**LOW**
		6.1 Property Crime Rates at Substation Area	LOW
		6.2 Substation Property Crime Incident last 5 years	LOW
7	The availability of other sources of energy to serve the load (e.g., customer owned back-up generation or storage solutions).	**7. Back Up Generation**	**LOW**
		7.1 Customer-Owned Back-up Generation	LOW
		7.2 Essential Loads with Back-up Generation	LOW
8	The availability of alternative ways to meet the health, safety, or security.	**8. Alternate Ways for Health, Safety, and Security**	**LOW**
		8.1 Condition of existing assets and structures	LOW
		8.2 Private Security Services	MID
		8.3 Additional measures to preserve Safety of Staff/Visitors	LOW
9	Requirements served by the load (e.g., back up command center or water storage facility).	**9. Critical Loads**	**LOW**
		9.1 Critical Loads	LOW

Table 5: Risk Index Results for Redacted

		[redacted] SUBSTATION	SUCCESSFUL PHYSICAL ATTACK Risk Index
1	The existing system resiliency and/or redundancy solutions (e.g., switching the load to another substation or circuit capable of serving the load, temporary circuit ties, mobile generation and/or storage solutions)	**1. Grid Resiliency**	LOW
		1.1 Capability of Switching the load to another substation	LOW
		1.2 Circuit Ties Capable of Serving the load	LOW
		1.3 Mobile Transformer	LOW
2	The availability of spare assets to restore a particular load.	**2. Spare Assets**	LOW
		2.1 Minimum Critical Spare Parts Stock on site	LOW
		2.2 Spare Parts Stock in a warehouse	LOW
3	The existing physical security protections to reasonably address the risk.	**3. Existing Physical Security**	LOW
		3.1 Concrete block masonry walls/Chain Link Fence	LOW
		3.2 Security Cameras	LOW
		3.3 Lighting	LOW
		3.4 Motion Detection	LOW
		3.5 Access Control	LOW
4	The potential for emergency responders to identify and respond to an attack in a timely manner.	**4. Emergency Responders**	LOW
		4.1 Local Police Agreement for Emergencies	MID
		4.2 Distance from police/fire dept. and time to respond	LOW
5	Location and physical surroundings, including proximity to gas pipelines and geographical challenges, and impacts of weather.	**5. Location**	LOW
		5.1 Geographical Challenges	LOW
		5.2 Impacts of Weather Events	LOW
6	History of criminal activity at the Distribution Facility and in the area.	**6. Criminal History**	LOW
		6.1 Property Crime Rates at Substation Area	LOW
		6.2 Substation Property Crime Incident last 5 years	LOW
7	The availability of other sources of energy to serve the load (e.g., customer owned back-up generation or storage solutions).	**7. Back Up Generation**	LOW
		7.1 Customer-Owned Back-up Generation	LOW
		7.2 Essential Loads with Back-up Generation	LOW
8	The availability of alternative ways to meet the health, safety, or security.	**8. Alternate Ways for Health, Safety, and Security**	LOW
		8.1 Condition of existing assets and structures	LOW
		8.2 Private Security Services	MID
		8.3 Additional measures to preserve Safety of Staff/Visitors	LOW
9	Requirements served by the load (e.g., back up command center or water storage facility).	**9. Critical Loads**	LOW
		9.1 Critical Loads	LOW

Table 6: Risk Index Results for Redacted

		[redacted] SUBSTATION	SUCCESSFUL PHYSICAL ATTACK Risk Index
1	The existing system resiliency and/or redundancy solutions (e.g., switching the load to another substation or circuit capable of serving the load, temporary circuit ties, mobile generation and/or storage solutions)	**1. Grid Resiliency**	**LOW**
		1.1 Capability of Switching the load to another substation	LOW
		1.2 Circuit Ties Capable of Serving the load	LOW
		1.3 Mobile Transformer	LOW
2	The availability of spare assets to restore a particular load.	**2. Spare Assets**	**LOW**
		2.1 Minimum Critical Spare Parts Stock on site	LOW
		2.2 Spare Parts Stock in a warehouse	LOW
3	The existing physical security protections to reasonably address the risk.	**3. Existing Physical Security**	**MID**
		3.1 Concrete block masonry walls/Chain Link Fence	LOW
		3.2 Security Cameras	MID
		3.3 Lighting	MID
		3.4 Motion Detection	LOW
		3.5 Access Control	MID
4	The potential for emergency responders to identify and respond to an attack in a timely manner.	**4. Emergency Responders**	**MID**
		4.1 Local Police Agreement for Emergencies	MID
		4.2 Distance from police/fire dept. and time to respond	LOW
5	Location and physical surroundings, including proximity to gas pipelines and geographical challenges, and impacts of weather.	**5. Location**	**LOW**
		5.1 Geographical Challenges	LOW
		5.2 Impacts of Weather Events	LOW
6	History of criminal activity at the Distribution Facility and in the area.	**6. Criminal History**	**MID**
		6.1 Property Crime Rates at Substation Area	MID
		6.2 Substation Property Crime Incident last 5 years	MID
7	The availability of other sources of energy to serve the load (e.g., customer owned back-up generation or storage solutions).	**7. Back Up Generation**	**LOW**
		7.1 Customer-Owned Back-up Generation	LOW
		7.2 Essential Loads with Back-up Generation	LOW
8	The availability of alternative ways to meet the health, safety, or security.	**8. Alternate Ways for Health, Safety, and Security**	**MID**
		8.1 Condition of existing assets and structures	LOW
		8.2 Private Security Services	MID
		8.3 Additional measures to preserve Safety of Staff/Visitors	MID
9	Requirements served by the load (e.g., back up command center or water storage facility).	**9. Critical Loads**	**LOW**
		9.1 Critical Loads	LOW

Table 7: Risk Index Results for Redacted

			SUCCESSFUL PHYSICAL ATTACK
	[redacted]		Risk Index
1	The existing system resiliency and/or redundancy solutions (e.g., switching the load to another substation or circuit capable of serving the load, temporary circuit ties, mobile generation and/or storage solutions)	**1. Grid Resiliency**	LOW
		1.1 Capability of Switching the load to another substation	LOW
		1.2 Circuit Ties Capable of Serving the load	LOW
		1.3 Mobile Transformer	LOW
2	The availability of spare assets to restore a particular load.	**2. Spare Assets**	LOW
		2.1 Minimum Critical Spare Parts Stock on site	LOW
		2.2 Spare Parts Stock in a warehouse	LOW
3	The existing physical security protections to reasonably address the risk.	**3. Existing Physical Security**	LOW
		3.1 Concrete block masonry walls/Chain Link Fence	LOW
		3.2 Security Cameras	LOW
		3.3 Lighting	LOW
		3.4 Motion Detection	LOW
		3.5 Access Control	LOW
4	The potential for emergency responders to identify and respond to an attack in a timely manner.	**4. Emergency Responders**	LOW
		4.1 Local Police Agreement for Emergencies	LOW
		4.2 Distance from police/fire dept. and time to respond	LOW
5	Location and physical surroundings, including proximity to gas pipelines and geographical challenges, and impacts of weather.	**5. Location**	LOW
		5.1 Geographical Challenges	LOW
		5.2 Impacts of Weather Events	LOW
6	History of criminal activity at the Distribution Facility and in the area.	**6. Criminal History**	LOW
		6.1 Property Crime Rates at Substation Area	LOW
		6.2 Substation Property Crime Incident last 5 years	LOW
7	The availability of other sources of energy to serve the load (e.g., customer owned back-up generation or storage solutions).	**7. Back Up Generation**	LOW
		7.1 Customer-Owned Back-up Generation	LOW
		7.2 Essential Loads with Back-up Generation	LOW
8	The availability of alternative ways to meet the health, safety, or security.	**8. Alternate Ways for Health, Safety, and Security**	LOW
		8.1 Condition of existing assets and structures	LOW
		8.2 Private Security Services	LOW
		8.3 Additional measures to preserve Safety of Staff/Visitors	LOW
9	Requirements served by the load (e.g., back up command center or water storage facility).	**9. Critical Loads**	LOW
		9.1 Critical Loads	LOW

VI. COVERED DISTRIBUTION FACILITY MITIGATION PLANS (STEP 1C)

Pursuant to the process identified in the Joint IOU/POU Straw Proposal and D.19-01-018, RPU has determined that the present level of risk at the four covered substations is not critical. However, there are some areas where the vulnerability of a physical attack to the facility could be improved.

All Mid-risk level cases were addressed with mitigation measures, and some Low-risk level cases, where the assessment identify room for improvements, also mitigation measures were presented, even though the risk was rated low.

These recommendations are discretionary and not mandatory for the security fitness of the substations. Appendix C contains a detail analysis of the recommended mitigating measures for these covered facilities. Table 8 below presents a summary of the mitigation measures per facility.

Table 8: Recommended Mitigation Measures. (Redacted)

[redacted]		[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	✓	✓	✓	✓

VII. INDEPENDENT EVALUATION AND RESPONSE (STEP 2)

A. REQUIREMENTS FOR QUALIFIED THIRD-PARTY REVIEW

D.19-01-018 specifies the following criteria for a Qualified Third-Party Reviewer:

Independence: A Qualified Third-Party Reviewer cannot be a division of the RPU. A governmental entity can select as the third-party reviewer another governmental entity within the same political subdivision, so long as the entity has the appropriate expertise, and is not a division of the POU that operates as a functional unit, i.e., a municipality could use its police department as its third-party reviewer if it has the appropriate expertise.

Adequate Qualifications: A Qualified Third Party Reviewer must be an entity or organization with electric industry physical security experience and whose review staff has appropriate physical security expertise, which means that it meets at least one of the following: (1) an entity or organization with at least one member who holds either an ASIS International Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization with demonstrated law enforcement, government, or military physical security expertise; or (3) an entity or organization approved to do physical security assessments by the CPUC, Electric Reliability Organization, or similar electrical industry regulatory body.

B. IDENTIFICATION OF THIRD-PARTY REVIEWER

RPU has selected as its Third-Party Reviewer AESI-US Inc. (AESI), an engineering and management consulting company based out of Atlanta Georgia. AESI's understanding of physical security for utility assets is founded in practical utility experience, and hands-on security implementation. AESI's Subject Matter Experts (SMEs) have significant experience in Threat, Risk and Vulnerability Assessments and Operational Security Audits, and progressive security and intelligence experience, as well as policies, procedures, access control systems, security incidents, emergency response planning and asset protection and implemented perimeter security solutions. AESI does not have any affiliation with Riverside Public Utilities or the City of Riverside.

The AESI team that conducted the third-party review was made up of the following three AESI resources:

- Loreto Sarracini, P.Eng. – President of AESI-US, Inc.
- Paul Stanley – AESI Senior Associate CPP (ASIS Certificate No# 8212)
- Carlos A. Mendizabal – President of ARETE Consulting Services Inc., AESI Senior Associate

The roles of the three team members were as follows:

- Carlos A. Mendizabal, conducted the physical security site visits at all identified Covered Distribution facilities and documented the findings.
- Loreto Sarracini, reviewed the findings from the physical walkdown conducted by Carlos along with the pictures of the Covered Distribution facilities and developed the first draft of the evaluation report.
- The evaluation report was then reviewed in detail by Carlos Mendizabal, and Paul Stanley.
- Paul Stanley conducted a thorough and detailed review of the evaluation report and provide Loreto Sarracini with his comments and assessments which were incorporated into the final evaluation report submitted to RPU.

Paul Stanley, AESI's senior associate, maintains the ASIS CPP certification (ASIS Certificate No# 8212). Paul's bio is presented below:

Paul Stanley, MSc, CPP

Paul has significant experience in Threat, Risk and Vulnerability Assessments and Operational Security Audits of significant properties and business facilities, including Workers Compensation environments. His practical knowledge covers all forms of facility management, physical and operational, with attention to system development and operational protection, specifically in terms of legal and compliance issues. Paul uses approved project management methods at critical infrastructure sites as recommended by the Project Management Institute (PMI) to ANSI standards, and maintains security clearances to 'Secret' with RCMP and Natural Resources Canada (NRCan). Paul understands the intricacies of the electrical power industry and the threats it incurs as society evolve through his work at BC Hydro and Alberta Electric System Operation (personnel and asset protection complying with industry and government standards).

Relevant Physical Security Experience

1. Conducted a comprehensive physical security assessment of the Duck River Electric Membership Corporation (DREMC) (Tennessee) of its corporate offices, district offices and substations and provided recommendations to improve the overall physical security posture.

2. Management of all aspects of the current Generation Security Program across British Columbia.

3. Operational direction of all security related matters at designated Generation NERC CIP sites.

4. International experience in security operations, information and intelligence gathering, political sensitivity, management interaction and close protection for individuals at risk.

5. Provided expertise is in the field of vulnerability, threat, and risk assessments, security, and life safety programs, including business continuity/crisis communications and

emergency and disaster management and the provision of suitable physical, operational, and technological countermeasures.

6. Direct responsibility for third-party risk and vulnerability assessments, security audits, business continuity/crisis management and emergency (including disaster) preparedness policies and recommendations, with clients situated in North America, Europe and both the Middle and Far East.

7. Responsibility to CEO and Executive with respect to all physical and operational security matters, including physical security for NERC CIP compliance.

C. PUBLIC RESULTS OF THIRD-PARTY EVALUATION

It is AESI's opinion that City of Riverside Public Utilities incorporate the changes the identified regarding the City of Riverside Public Utilities Physical Security Plan (PSP) report. The recommended changes are not a requirement and do not preclude AESI from agreeing with findings of the PSP.

RPU's Third-Party reviewer, AESI has reviewed the Physical Security Plan developed by Riverside Public Utility and the following is a public summary of the conclusion and recommendations.

The PSP describes RPU's risk management approach toward distribution system physical security, factoring in the appropriate consideration of resiliency, impact, and cost.

RPU conducted a detailed assessment of their distribution facilities to identify the "Covered" Distribution facilities that may merit special protection. For each one of the identified Covered Distribution facilities, RPU conducted a comprehensive physical security risk assessment to identify any potential threats and vulnerabilities and identified the associated mitigation measures to address the identified threats and vulnerabilities. The physical security risk assessment factored in existing grid resiliency, available back-up generation, spare parts and redundance to supply for the critical loads.

Although, RPU has strong resilience due to the redundant characteristic of their electrical distribution system, the strong redundant will help minimize the impact of a potential outage causes by a physical attack but will not minimize a potential physical attack from occurring.

In AESI's review of the PSP, several additional observations were made with regards to processes, people and technology as it relates to physical security which RPU should consider implementing. The suggested recommendations focus on strengthening RPU's physical security program to deter an event from occurring that could lead to an outage. It was also observed that in some cases, if there is no history of an event occurring then the risk of one occurring in the future is considered low and therefore, no additional physical security measures were identified. Even though an event has not occurred, it was also suggested that RPU, consider implementing the suggested physical security measures to be prepared if the event were to occur in the future.

The following is a summary of the observations and suggested recommendations (Redacted):

D. RIVERSIDE PUBLIC UTILITIES RESPONSE

RPU has reviewed the comments and mitigations proposed by AESI. RPU agrees that strong resiliency will not minimize a potential physical attack from occurring. The Covered Distribution facilities have sufficient physical security infrastructure in place to keep the risk level of all facilities at a low level. The following is a response to the points raised by AESI.

Redacted

VIII. VALIDATION (STEP 3)

A. SELECTION OF QUALIFIED AUTHORITY

RPU submitted its Physical Security Plan to Riverside Police Department (RPD) for further review and validation. RPD evaluated and validated the plan.

B. PLAN AS ADEQUATE.RESULTS OF QUALIFIED AUTHORITY REVIEW

MEMO

Police Department

DATE: August 3, 2021

TO: FADY MEGALA, PRINCIPAL ENGINEER, PUBLIC UTILITIES DEPARTMENT
FROM: LARRY V. GONALEZ, CHIEF OF POLICE, POLICE DEPARTMENT
CC: CHRIS WAGNER, POLICE CAPTAIN; STEVE GOODSON, POLICE LIEUTENANT

RE: Physical Security Plan for RPU facilities

The Riverside Police Department has reviewed the physical security plans, prepared by Eric Hartman representing Power Tech Engineers (PTEI), for the following Riverside Public Utilities (RPU) facilities:

[redacted]

The Police Department agrees with the 'Recommended Mitigation Measures' listed in ***'Appendix C: Mitigation Plan in Table 1: Mitigation Measures for the Covered Substations'***. An identical table is also included in the body of the Riverside Public Utilities Power Utility Security Plan on Page 20. The Riverside Police Department agrees that the recommendations in this table would assist RPU in safeguarding the above listed facilities.

Larry V. Gonzalez
Chief of Police
Riverside Police Department

IX. ADOPTION (STEP 4)

The RPU Physical Security Plan will be presented to the Board pf Public Utilities and to the Council for adoption.

X. MAINTENANCE (STEP 5)

RPU will refine and update its Physical Security Plan as appropriate and as necessary to preserve the plan integrity.

XI. REPEAT PROCESS (STEP 6)

RPU will repeat this six step process at least once every five years.