ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

RESPONSE DUE:

Within I hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met.

Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met.

By the later of 24 hours after the recognition of the incident OR by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. Note 4 00pm local time will be considered the end of the business day

Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident.

For NERC reporting entities registered in the United States, NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.

METHODS OF FILING RESPONSE

(Retain a completed copy of this form for your files.)

Online:

Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/

FAX:

FAX Form OE-417 to the following facsimile number: (202) 586-8485.

Alternate:

If you are unable to submit online or by fax, forms may be e-mailed to doehgeoc@ha doe gov, or call and report the information to the

following telephone number: (202) 586-8100.

SCHEDULE 1 -- ALERT CRITERIA

(Page I of 4)

Criteria for Filing (Check all that apply) See Instructions For More Information

1. Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations 2. [X] Cyber event that causes interruptions of electrical system operations EMERGENCY ALERT 3. [] Complete operational failure or shut-down of the transmission and/or distribution electrical system File within 1-Hour 4. [] Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise If any box 1-8 on the right is blacked out area or within the partial failure of an integrated electrical system checked, this form must be filed within 1 hour of the 5. [] Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident, check Emergency Alert (for the Alert Status) on Line A below. 6. [] Firm load shedding of 100 Megawatts or more implemented under emergency operational policy 7. [] System-wide voltage reductions of 3 percent or more 8. [] Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System NORMAL REPORT 9. [] Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which File within 6-Hours targets components of any security systems If any box 9-12 on the right is checked AND none of the 10. [X] Cyber event that could potentially impact electric power system adequacy or reliability boxes 1-8 are checked, this form must be filed within 6 11. [] Loss of electric service to more than 50,000 customers for 1 hour or more hours of the incident, check Normal Report (for the Alert 12. [] Fuel supply emergencies that could impact electric power system adequacy or reliability Status) on Line A below.

ביין און און אין אין אין אין אין אין אין אין אין אי						IU DUE				
			SCHEI	OULE 1 A	LERT CRI	TERIA C	ONTINUE	D		
		13. [1 Damage or destru	tion of a Facility wi	tion of a Facility within its Reliability Coordinator Area, Balancing Authority Area or					
		15.				id a Bulk Electric Sys				
		14. [] Damage or destru	ction of its Facility th	at results from actu	al or suspected intent	ional human action.			
		15. [nt to its Facility excluding weather or natural disaster related threats, which has the potential to formul operation of the Facility. Or suspicious device or activity at its Facility.						
	STEM REPORT thin 1-Business Day	16. [] Physical threat to has the potential t Electric System c	o degrade the normal	tem control center, e I operation of the co	excluding weather or ntrol center. Or suspi	natural disaster relat cious device or activ	ed threats, which city at its Bulk		
If any box 13-24 on the right is checked AND none of the boxes 1-12 are checked, this form must be filed by the later of 24 hours after the recognition of the incident OR by the end of the next business day. Note 4:00pm local time will be considered the end of the business day. Check System Report (for the Alert		17. [System Emergency resulting in voltage deviation on a Facility; A voltage deviation equal to or 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.						
		18, [18. [] Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts							
		19. [19. [] Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.							
		20. [Complete loss of Requirements.	off-site power (LOO)	P) affecting a nuclea	ar generating station j	per the Nuclear Plan	t Interface		
Status) on Line A below. 21. [] Unexpected Transcription Facilities caused] Unexpected Trans Facilities caused !	mission loss within to by a common disturb	its area, contrary to cance (excluding suc	design, of three or mo cessful automatic rec	ore Bulk Electric Systems (1981).	stem		
		22. [] Unplanned evacua	nation from its Bulk Electric System control center facility for 30 continuous minutes or more.						
		23. [] Complete loss of its staffed Bulk E	Interpersonal Communication and Alternative Interpersonal Communication capability affecting Electric System control center for 30 continuous minutes or more.						
		24. [] Complete loss of continuous minut	monitoring or control capability at its staffed Bulk Electric System control center for 30 tes or more.						
If signifi	cant changes have occur	red after	filing the initial repo	rt, re-file the form w	ith the changes and	check Update (for the	e Alert Status) on Li	ne A below.		
The form	nust be re-filed within	72 hour	s of the incident with	the latest information	n and Final (Alert Si	tatus) checked on Lis	ie A below, unless u	pdated		
LINE										
NO.						r				
A.	Alert Status (check one	•)		Emergency Alert [X] 1 Hour	Normal Report [] 6 Hours	System Report [] 1 Business Day	Update [] As required	Final [] 72 Hours		
В.	Organization Name		WHAT - 1	sPower	<u> </u>		<u> </u>			

2180 South 1300 East Suite 600 Salt Lake City Utah 84106

C.

Address of Principal Business Office

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

S	CHED	TIT	H	1 .	Δ	TER	T ?	OV	TT	CF

(Page 3 of 4) INCIDENT AND DISTURBANCE DATA California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County; Geographic Area(s) Affected D. (County, State) 03 - 05 - 2019 / 09 : 12 no dd yy hh mm] Eastern] Central [X] Mountain Date/Time Incident Began E.] Pacific Alaska] Hawaii (mm-dd-yy/hh mm) using 24-hour clock [X] Mountain] Central Date/Time Incident Ended <u>03 - 05 - 2019 / 18 : 57</u>] Eastern F. Pacific Alaska [] Hawaii hh (mm-dd-yy/ hh:mm) using 24-hour clock mo dd уу mm Did the incident/disturbance originate in your Unknown [X] Yes [] G. No[] system/area? (check one) Estimate of Amount of Demand Involved Zero [X] Unknown [] H. (Peak Megawatts) Unknown [Zero [X] I. Estimate of Number of Customers Affected

J. Cause K. Impact L. Action Taken None	SCHEI	DULE 1 – TYPE OF EMERGEN	CY
None Control center loss, failure, or evacuation Loss or degradation of control center monitoring or communication systems Damage or destruction of a facility Electrical system separation (islanding) None Shed Firm Load: Load shedding of 100 Major triansmission and/or distribution system Major triansmission systems interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major triansmission systems interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more Loss of electric service to more than 50,000 customers for 1 hour or more System-wide voltage reductions or 3 percent or more System-wide voltage reductions or 3 percent or more System voltage reductions or 3 percent or more Spot Interruptible Load Repaired or restored Mitigation implemented Other Additional Information/Comments Additional Information/Comments Additional Information/Comments Steparate or committed to remove the exposed vibrage to remove the exposed vibracability Additional Information/Comments Spot Interruptible Load Spot Inte			T Assiss Talian
Control center loss, failure, or evacuation Loss or degradation of control center monitoring or communication systems Damage or destruction of a facility Electrical system separation (islanding) Complete operational failure or shutdown of the transmission and/or distribution system Major transmission system interruption (three or more BES elements) Cyber event (information technology) Cyber event (operational technology) Fuel supply emergencies, interruption, or deficiency Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure Transmission equipment failure (not including substation or switchyard) Failure at high voltage substation or switchyard Weather or natural disaster Operator action(s) Other Additional Information/Comments: Initial assessment emedet that a firewell explais was likely usified to esercting a definity of sentence in the addition of switch and the firewell explais was likely usified to esercting a definition of switch greated for the swells to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoils to reduce the search as definited of swords at stack that caused the fivewoil to reduce the search as definited of swords at stack that caused the fivewoil to reduce the search as definited of swords at stack that caused the fivewoil to reduce the swords and between the definition and between the substantial states and between the swords and between the state of the swords at the sword and between the state of the swords at the sword and between the swo	J. Cause	K. Impact	L. Atlun Taken
	□ Physical attack □ Threat of physical attack □ Vandalism □ Theft □ Suspicious activity □ Cyber event (information technology) □ Cyber event (operational technology) □ Fuel supply emergencies, interruption, or deficiency □ Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure □ Transmission equipment failure (not including substation or switchyard) □ Failure at high voltage substation or switchyard □ Weather or natural disaster □ Operator action(s) □ Other ■ Additional Information/Comments: Initial assessment revealed that a firewall exploit was likely utilized to execute a denial of service attack that caused the firewalls to reboot	 □ Control center loss, failure, or evacuation □ Loss or degradation of control center monitoring or communication systems □ Damage or destruction of a facility □ Electrical system separation (islanding) □ Complete operational failure or shutdown of the transmission and/or distribution system □ Major transmission system interruption (three or more BES elements) □ Major distribution system interruption □ Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more □ Loss of electric service to more than 50,000 customers for 1 hour or more □ System-wide voltage reductions or 3 percent or more □ Voltage deviation on an individual facility of ≥10% for 15 minutes or more □ Inadequate electric resources to serve load □ Generating capacity loss of 1,400 MW or more □ Generating capacity loss of 2,000 MW or more □ Complete loss of off-site power to a nuclear generating station ☑ Other ☑ Additional Information/Comments: Firewall reboots resulted in brief communications outages (approximately 5 minutes) between field devices at sites and between 	Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system Implemented a warning, alert, or contingency plan Voltage reduction Shed Interruptible Load Repaired or restored Mitigation implemented Other Additional Information/Comments Alter leaming of the potential cause of the reboot, aPower started besting and deployment of an update to remove the

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

SCHEDULE 2 - NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or

		ad as United Energy Infrastricture information.
NAME OF OFFI	CIAL THAT SHOULD BE	CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION
M. Name	Lu	cas Root
N. Title	Dir	ector, Operations
O. Telephone Number	(80)	1)-(679)-(3527)
P. FAX Number	() ()()
Q. E-mail Address		of@spower.com
mitigation actions taken, equipmen investigations. Be sure to identify: electrical system separation (and if (shown by capacity type and voltag be spoolied to meet the requirement:	it damaged, critical infrastru the estimate restoration date there were, what the islandi ge size grouping). If necessary this includes the NERC EOP-C box on line A for Alert Status	e it. Include as appropriate, the cause of the incident/disturbance, change in frequency, ctures interrupted, effects on other systems, and preliminary results from any of the name of any lost high voltage substations or switchyards, whether there was any no boundaries were), and the name of the generators and voltage lines that were lost of the company and attach additional sheets. Equivalent documents, containing this information can 104 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule 1 on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours
R. Narrative:	A contract of the contract of	
This information will be provided in a sub-	sequent update after additional inf	ormation gathering
S. Estimated Restoration Date for	all Affected Customers	
Who Can Receive Power		mo dd yy-
	Pioneer, Beacon 4, ABS	SR, DSR1, DSR2, Beacon 1, Elevation C, WABSRB, Bayshore A, Bayshore B, Bayshore C, and Solverde.

U. Notify NERC/E-ISAC

If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc.net and/or operations@cisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC.

☑ Notify NERC | ☑ Notify E-ISAC

Document 2

DIGIZO 17 J.JO.OU FINI JODININGEO TO EACH

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE 417

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

RESPONSE DUE:

Within I hour of the incident, submit Schedule I and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met.

Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met.

By the later of 24 hours after the recognition of the incident <u>OR</u> by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. Note 4 00pm local time will be considered the end of the business day

Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident.

For NERC reporting entities registered in the United States; NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.

METHODS OF FILING RESPONSE

(Retain a completed copy of this form for your files.)

Online:

Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/

FAX:

FAX Form OE-417 to the following facsimile number: (202) 586-8485.

Alternate:

If you are unable to submit online or by fax, forms may be e-mailed to doehgeoc@hq.doe.gov, or call and report the information to the

following telephone number: (202) 586-8100.

SCHEDULE 1 -- ALERT CRITERIA

(Page 1 of 4)

Criteria for Filing (Check all that apply)

See Instructions For More Information									
	1. [] Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations								
	2. [X] Cyber event that causes interruptions of electrical system operations								
EMERGENCY ALERT File within 1-Hour	3. [] Complete operational failure or shut-down of the transmission and/or distribution electrical system								
If any box 1-8 on the right is checked, this form must be	4. [] Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system								
filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on	5. [] Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident								
Line A below.	6. [] Firm load shedding of 100 Megawatts or more implemented under emergency operational policy								
	7. [] System-wide voltage reductions of 3 percent or more								
	8. [] Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System								
NORMAL REPORT File within 6-Hours	9. [] Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems								
If any box 9-12 on the right is checked AND none of the	10. [X] Cyber event that could potentially impact electric power system adequacy or reliability								
boxes 1-8 are checked, this form must be filed within 6	11. [] Loss of electric service to more than 50,000 customers for 1 hour or more								
hours of the incident; check Normal Report (for the Alert Status) on Line A below.	12. [] Fuel supply emergencies that could impact electric power system adequacy or reliability								

			SCHEI	OULE 1 A	LERT CRI (Page 2 of	ITERIA C	CONTINUE	D	
		13. [J Damage or destrue Transmission Ope	ction of a Facility wi rator Area that result	thin its Reliability C	Coordinator Area, Ba id a Bulk Electric Sy	lancing Authority Ar stem Emergency.	ea or	
		14. [] Damage or destruction of its Facility that results from actual or suspected intentional human action.							
		15. [] Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.							
	STEM REPORT thin 1-Business Day	16. [Physical threat to has the potential t Electric System c	o degrade the norma	tem control center, of the co	excluding weather or outrol center. Or susp	natural disaster rela icious device or acti	ted threats, which vity at its Bulk	
check	ox 13-24 on the right is ed AND none of the 1-12 are checked, this	17. [] Bulk Electric System Emergency resulting in voltage deviation on a Facility; A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.							
form m of	ist be filed by the later 24 hours after the	18. I Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts							
by the e	ion of the incident <u>OR</u> ad of the next business to 4:00pm local time	19. [] Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.							
the b System	will be considered the end of the business day. Check System Report (for the Alert		20. [] Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements.						
Statu	s) on Line A below.	21. [] Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).							
		22. [] Unplanned evacu	ation from its Bulk E	lectric System contr	rol center facility for	30 continuous minu	tes or more.	
		23. [native Interpersonal (innous minutes or m		bility affecting	
		24. [monitoring or control capability at its staffed Bulk Electric System control center for 30 test or more.					
If signifi	cant changes have occur	red after	filing the initial repo	rt, re-file the form w	ith the changes and	check Update (for th	e Alert Status) on Li	пе A below.	
The form	ı must be re-filed within	72 hour	s of the incident with	the latest informatio	n and Final (Alert S	tatus) checked on Li	ne A below, unless u	pdated	
LINE NO.							A GREEN CONTRACTOR		
A.	Alert Status (check one	;)		Emergency Alert [] 1 Hour	Normal Report [] 6 Hours	System Report [] 1 Business Day	Update [X] As required	Final [] 72 Hours	
В.	Organization Name		sPower		İ	L.			
				2400 Coult 4200	Eart Cuita BOO C	alt Laka City Litah	24106		
				2100 50001 1300	Casi Suite 600 Si	alt Lake City Utah (JH 100		
C. Address of Principal Business Office									

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

SCHEDULE 1 ALERT NOTIC	S	CHEDUI	E	1.	AT	ERT	٦٦	ΙО,	TIC	Ŧ	3
------------------------	---	--------	---	----	----	-----	----	-----	-----	---	---

(Page 3 of 4) INCIDENTIAND DISTURBANCE DATA California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County; Geographic Area(s) Affected D. (County, State) [X] Mountain 03 - 05 - 2019 / 09 : 12 no dd yy hh mm] Eastern] Central Date/Time Incident Began E. 1 Pacific] Alaska Hawaii (mm-dd-yy/hh:mm) using 24-hour clock] Central [X] Mountain] Eastern Date/Time Incident Ended 03 - 05 - 2019 / 18 : 57 F. dd Pacific Alaska [] Hawaii (mm-dd-yy/ hh:mm) using 24-hour clock hh УУ mm Did the incident/disturbance originate in your Unknown [X] Yes [] No[] G. system/area? (check one) Estimate of Amount of Demand Involved Zero [X] Unknown [] H. (Peak Megawatts) Unknown [Zero [X] Estimate of Number of Customers Affected I.

SCHEDULE 1 – TYPE OF EMERGENCY										
	Check all that apply									
J. Cause	K. Impact	L. Action Taken								
□ Unknown □ Physical attack □ Threat of physical attack □ Vandalism □ Theft □ Suspicious activity □ Cyber event (information technology) ☑ Cyber event (operational technology) □ Fuel supply emergencies, interruption, or deficiency □ Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure □ Transmission equipment failure (not including substation or switchyard) □ Failure at high voltage substation or switchyard □ Weather or natural disaster □ Operator action(s) □ Other ☑ Additional Information/Comments: Initial assessment revealed that a firewall exploit was likely utilized to execute a denial of service attack that caused the firewalls to reboot leading to an approximately 5 minute communications outage	 □ None □ Control center loss, failure, or evacuation □ Loss or degradation of control center monitoring or communication systems □ Damage or destruction of a facility □ Electrical system separation (islanding) □ Complete operational failure or shutdown of the transmission and/or distribution system □ Major transmission system interruption (three or more BES elements) □ Major distribution system interruption □ Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more □ Loss of electric service to more than 50,000 customers for 1 hour or more □ System-wide voltage reductions or 3 percent or more □ Voltage deviation on an individual facility of ≥10% for 15 minutes or more □ Inadequate electric resources to serve load □ Generating capacity loss of 1,400 MW or more □ Generating capacity loss of 1,400 MW or more □ Complete loss of off-site power to a nuclear generating station ☑ Other ☑ Additional Information/Comments: Firewall reboots resulted in brief communications outages (approximately 5 minutes) between field devices at sites and between the sites and sPower's Control Center 	□ None □ Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) □ Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system □ Implemented a warning, alert, or contingency plan □ Voltage reduction □ Shed Interruptible Load □ Repaired or restored □ Mitigation implemented ☑ Other ☑ Additional Information/Comments After learning of the potentias cause of the reboot, sPower started testing and deployment of an update to remove the exploited vulnerability								

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

SCHEDULE 2 - NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g.,

	exemptions for confidential comm	cial information and trade secrets, certain information that could endanger the physical safety of an individual, information designated as Critical Energy Infrastructure Information.	
	NAME OF OFFICE	L THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION	
M.	Name	Lucas Root	
N.	Title	Director, Operations (801)-(679)-(3527)	
O. P.	Telephone Number FAX Number	(001)-(014)-(0021)	
O.	E-mail Address	Iroot@spower.com	
mitig inves electi (shov be su need after R. ?	ation actions taken, equipment or tigations. Be sure to identify: the rical system separation (and if the synthesis of the sure of the sure of pplied to meet the requirement; the synthesis of the final book detection that a criterion was me Narrative:	d actions taken to resolve it. Include as appropriate, the cause of the incident/disturbance, change in frequency maged, critical infrastructures interrupted, effects on other systems, and preliminary results from any estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was e were, what the islanding boundaries were), and the name of the generators and voltage lines that were leavening. If necessary, copy and attach additional sheets. Equivalent documents, containing this information includes the NERC EOP-004 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule and line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 horeoperator of wind and solar generation assets that are operated from a Control Center in Salt Lake City, UT. (b) (7)(E) These updates are ongoing.	any ost ion can lule I
25071	itimated Restoration Date for all ho Can Receive Power	Hected Customers — dd yy	
		Pioneer, Beacon 4, ABSR, DSR1, DSR2, Beacon 1, Elevation C, WABSRB, Bayshore A, Bayshore B, Bayshore C, Solv	erde,
T, N	ame of Assets Impacted	Brewall at sPower headquarters	
U.N	otify NERC/E-ISAC	Select if you approve of all of the information provided on the Form being submitted to the North America Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (E-IS.) NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce a standards for the bulk power system but that is not part of the Federal Government. This information we submitted to help fulfill the respondent's requirements under NERC's reliability standards. If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc ne operations@eisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these by NERC and/or E-ISAC.	AC) eliability uld be t and/or

Document 3

From:

Tarduogno, Matthew

To:

Evans, Karen S; Lotto, Adrienne

Cc: Subject: Kenneth Buell (Kenneth.Buell@hq.doe.gov); Kumar, Puesh

Date:

Follow-Up on Denial of Service Incident Friday, March 08, 2019 5:59:00 PM

OFFICIAL USE ONLY

All,

I wanted to quickly follow-up on the denial-of-service (DoS) incident experienced by sPower, a company that owns and operators solar and wind generation assets in several states, that we noted this morning. I spoke with the operations manager of sPower this morning and the E-ISAC has also been in contact with the company.

On March 5, sPower noted a series of brief communication outages between their control center and their remote sites. Upon further investigation, the communications outages were determined to have been caused by firewall reboots. After consulting with Cisco, the firewall manufacture, it was determined that the firewall reboots were caused by a DoS attack exploding a known vulnerability. Cisco recommended a firmware update, which sPower has been deploying across their system, after testing for compatibility. The DoS incdent was observed intermittently over a 12 hour period and no further activity has been observed since this time. sPower has reviewed log files and has found no evidence of a breach beyond the DoS attack. Additionally, the incident did not have any impacts on operations.

When I spoke with sPower they did not expect to need any additional support or have any ongoing concerns; however, they will contact us if there are any issues. (b) (7)(E)

We have been providing DOE's Office of Intelligence and

Counterintelligence with updates and they are ready to investigate any indicators, as appropriate, and have been checking for any related incidents. We will work with IN and the ISACs to provide appropriate information to the sector as available.

Please let me know if you have any questions.

Best Regards,

-Matt

Matthew T. Tarduogno

Infrastructure Security & Energy Restoration

Office of Cybersecurity, Energy Security, & Emergency Response

U.S. Department of Energy

Office: 202-586-2892 | Mobile: (b) (6)

Matthew.Tarduogno@hq.doe.gov

OFFICIAL USE ONLY

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

RESPONSE DUE:

Within 1 hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met.

Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met.

By the later of 24 hours after the recognition of the incident OR by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. Note 4 00pm local time will be considered the end of the business day

Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident.

For NERC reporting entities registered in the United States; NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.

METHODS OF FILING RESPONSE

(Retain a completed copy of this form for your files.)

Online:

Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/

FAX:

FAX Form OE-417 to the following facsimile number: (202) 586-8485.

Alternate:

If you are unable to submit online or by fax, forms may be e-mailed to dochgeoc@hq.doe.gov, or call and report the information to the

following telephone number: (202) 586-8100.

SCHEDULE 1 -- ALERT CRITERIA

(Page 1 of 4)

Criteria for Filing (Check all that apply) See Instructions For More Information 1. Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations

2. [X] Cyber event that causes interruptions of electrical system operations EMERGENCY ALERT

3. [] Complete operational failure or shut-down of the transmission and/or distribution electrical system

If any box 1-8 on the right is checked, this form must be filed within I hour of the incident, check Emergency Alert (for the Alert Status) on Line A below.

File within 1-Hour

-] Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system
- 5. Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single
- 6. Firm load shedding of 100 Megawatts or more implemented under emergency operational policy
- 7. [] System-wide voltage reductions of 3 percent or more
- 8. [] Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System

NORMAL REPORT File within 6-Hours

If any box 9-12 on the right is checked AND none of the boxes 1-8 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert

Status) on Line A below.

- 9. [] Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems
- 10. [X] Cyber event that could potentially impact electric power system adequacy or reliability
- 11. Loss of electric service to more than 50,000 customers for 1 hour or more
- 12. [] Fuel supply emergencies that could impact electric power system adequacy or reliability

			SCHEI	DULE 1 ALERT CRITERIA CONTINUED (Page 2 of 4)						
		13. [] Damage or destru Transmission Ope	ction of a Facility wi rator Area that result	thin its Reliability C is in action(s) to avo	oordinator Area, Bal id a Bulk Electric Sy	ancing Authority Ar stem Emergency.	ea or		
		14. [] Damage or destru	ruction of its Facility that results from actual or suspected intentional human action.						
•		15. [] Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.								
	STEM REPORT thin 1-Business Day	16. [] Physical threat to its Bulk Electric System control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. Or suspicious device or activity at its Bulk Electric System control center.								
check	ex 13-24 on the right is ed AND none of the 1-12 are checked, this	17. [17. [] Bulk Electric System Emergency resulting in voltage deviation on a Facility; A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.							
form m of	ist be filed by the later 24 hours after the ion of the incident OR	18. [] Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts								
by the edday. No	nd of the next business to 4:00pm local time considered the end of	19. [19. [] Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.							
the b System	usiness day. Check Report (for the Alert s) on Line A below.	20. [] Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements.								
Jau	ou line A ollow.	21. [] Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).								
22. [] Unplanned evacu			ation from its Bulk F	lectric System contr	ol center facility for	30 continuous minu	tes or more.			
				Interpersonal Communication and Alternative Interpersonal Communication capability affecting Electric System control center for 30 continuous minutes or more.						
		24. [] Complete loss of continuous minut	monitoring or control capability at its staffed Bulk Electric System control center for 30 tes or more.						
If signifi	cant changes have occur	red after	filing the initial repo	ort, re-file the form w	ith the changes and	check Update (for th	e Alert Status) on Li	ne A below.		
	nust be re-filed within	72 hour	s of the incident with	the latest informatio	n and Final (Alert S	atus) checked on Li	ne A below, unless u	pdated		
LINE NO.		- 50								
A.	Alert Status (check one	:)		Emergency Alert [] I Hour	Normal Report [] 6 Hours	System Report [] 1 Business Day	Update [] As required	Final [X] 72 Hours		
В.	Organization Name			sPower						
C.	Address of Principal B	Office	2180 South 1300	East Suite 600 Sa	ilt Lake City Utah 8	4106				

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

S	CHEDI	$\Pi \mathbf{F}$	1	ALER	ו ד	VO	TT	C	ľ
. 7		1 1 1 1 2		- 1 I I I I I I I I I I I I I I I I I I		71 1	, , ,	١.	

(Page 3 of 4)										
INCIDENT AND DISTURBANCE DATA										
D.	Geographic Area(s) Affected (County, State)	California: Kern County, Los Angeles	County; Utah: Salt Lak	e County; Wyoming	g: Converse County;					
E.	Date/Time Incident Began (mm-dd-yy/hh mm) using 24-hour clock	_03 - 05 - 2019 / 09 : _ mo dd yy hh i	12 [] Eas nm [] Pac	tem []Cea ific []Ala	ska [] Hawaii					
F.	Date/Time Incident Ended (mm-dd-yy/ hh:mm) using 24-hour clock	_03 - 05 - 2019 / 18 : mo dd yy hh i	_57 [] Eas mn [] Pac		., .					
G.	Did the incident/disturbance originate in your system/area? (check one)	Yes []	No []		Unknown [X]					
H.	Estimate of Amount of Demand Involved (Peak Megawatts)		Zero [X]		Unknown []					
I.	Estimate of Number of Customers Affected		Zero [X]		Unknown []					

Check all that apply	SCHEDULE 1 – TYPE OF EMERGENCY				
None Control center loss, failure, or evacuation Loss or degradation of control center monitoring or communication systems Damage or destruction of a facility Electrical system separation (islanding) None Shed Firm Load: Load shedding of 100 Major transmission and/or distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) Major distribution system interruption (three or more BES elements) More more of firm system loads for 15 minutes or more Decented to severally via UFLS or remedial action scheme) Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system Implemented a warning, alert, or contingency plan Voltage reduction Implemented Woltage redu	Check all that apply				
Control center loss, failure, or evacuation Loss or degradation of control center monitoring or communication systems Damage or destruction of a facility Electrical system separation (Islanding) Complete operational failure or shutdown of the transmission and/or distribution system Major transmission system interruption (three or more BES elements) Cyber event (information technology) Cyber event (operational technology) Fuel supply emergencies, interruption, or deficiency Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure Transmission equipment failure (not including substation or switchyard) Failure at high voltage substation or switchyard Weather or natural disaster Operator action(s) Other Additional Information/Comments: Interruption of servent expect was alway utilized to escending a dorsing to an approximately 5 mirrole or less communications outage (page) Additional Information/Comments: Firewall rebooks resulted in brief communications outages (page) Additional Information/Comments: Firewall rebooks resulted in brief communications outages (page) Additional Information/Comments: Firewall rebooks resulted in brief communications as these and	J. Cause	K. Impact	L. Action Taken		
	□ Physical attack □ Threat of physical attack □ Vandalism □ Theft □ Suspicious activity □ Cyber event (information technology) ⊠ Cyber event (operational technology) □ Fuel supply emergencies, interruption, or deficiency □ Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure □ Transmission equipment failure (not including substation or switchyard) □ Failure at high voltage substation or switchyard □ Weather or natural disaster □ Operator action(s) □ Other ☑ Additional Information/Comments: Initial assessment revealed that a firewall exploit was fixely utilized to execute a derial of service attack that caused the firewalls to reboot	 □ Control center loss, failure, or evacuation □ Loss or degradation of control center monitoring or communication systems □ Damage or destruction of a facility □ Electrical system separation (islanding) □ Complete operational failure or shutdown of the transmission and/or distribution system □ Major transmission system interruption (three or more BES elements) □ Major distribution system interruption □ Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more □ Loss of electric service to more than 50,000 customers for 1 hour or more □ System-wide voltage reductions or 3 percent or more □ Voltage deviation on an individual facility of ≥10% for 15 minutes or more □ Inadequate electric resources to serve load □ Generating capacity loss of 1,400 MW or more □ Generating capacity loss of 2,000 MW or more □ Complete loss of off-site power to a nuclear generating station ☑ Other ☑ Additional Information/Comments: Firewall reboots resulted in brief communications outages (approximatery 5 minutes or less) between field devices at sites and 	Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system Implemented a warning, alert, or contingency plan Voltage reduction Shed Interruptible Load Repaired or restored Mitigation implemented Other Additional Information/Comments After learning of the potential cause of the reboot, sPower started testing and deployment of an update to remove the		

ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT

OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

SCHEDULE 2 – NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.

exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.			
NAME OF OFFICIAL THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION			
M.	Name	Lucas Root	
N.	Title	Director, Operations	
O.	Telephone Number	(801)-(679)-(3527)	
P.	FAX Number	(x,y)	
Q.	E-mail Address		
mitiga investi electri (show be sup needs	tion actions taken, equipment dan gations. Be sure to identify: the o cal system separation (and if ther n by capacity type and voltage siz plied to meet the requirement; this i	maged, critical infrastructures interrupted, effects on other systems, and preliminary results from any estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was any e were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost e grouping). If necessary, copy and attach additional sheets. Equivalent documents, containing this information can includes the NERC EOP-004 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule 1 on line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours	
D A			
	rralive:		
SPOW(9	is a Generator Owner and Generator C	perator of wind and solar generation assets that are operated from a Control Center in Salt Lake City, UT: (b) (7)(E)	
20.12.11.11.11.1			
S. Estimated Restoration Date for all Affected Customers Who Can Receive Power mo dd yy			
		Pioneer, Beacon 4, ABSR, DSR1, DSR2, Beacon 1, Elevation C, WABSRB, Bayshore A, Bayshore B, Bayshore C, Solverde, firewall at sPower headquarters	
T. Nar	ne of Assets Impacted		
Select if you approve of all of the information provided on the Form being submitted to the North Ame Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (I			
U. Notify NERC/E-ISAC	NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk power system but that is not part of the Federal Government. This information would be submitted to help fulfill the respondent's requirements under NERC's reliability standards.		
	ity NERC/E-ISAC	If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc.net and/or operations@eisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC.	
		Notify NERC M Notify E-ISAC	