NESCOR Cybersecurity Failure Scenarios Evaluation Sheet

Group Name:

Scenario	AMI.9 Invalid Disconnect Messages to Meters Impact Customers and Utility				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	AMI.32 Power Stolen by Reconfiguring Meter via Optical Port				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DER.7 Incorrect Clock Causes Substation DER System Shut Down During Critical Peak				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DER.16 DER SCADA System Issues Invalid Commands				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DER.20 Compromised DERMS Weather Data Modifies DER Output Forecasts				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	WAMPAC.6 Compromised Communications between PMUs and Control Center				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	ET.16 An EV is Exploited to Threaten Transformer or Substation				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DR.1 Blocked DR Messages Result in Increased Prices or Outages				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DR.4 Improper DRAS Configuration Causes Inappropriate DR Messages				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9

Scenario	DGM.6 Spoofed Substation Field Devices Influence Automated Responses				
Impact	0	1	3	7	9
Adversary Cost	0.1	1	3	7	9