



<b>Title: Aurora Mitigation Plan</b>	
<b>File Name: OMU Aurora Mitigation Plan v10 01-01-18</b>	
<b>Version: 10</b>	<b>Page: 1 of 12</b>
<b>Effective Date: 1/1/2018</b>	<b>Review Frequency: As Needed</b>

Title			
Aurora Mitigation Plan			
Version	Effective Date	Review Frequency	
10	1/1/2018	As Needed	
Business Unit	Department	Section	
Delivery (DEL)	DEL - Compliance	DEL - NERC	
Type of Change	Access	Other Dep't Affected	Retention
Change - See Revision Section	Restricted	Yes - See Section 2.0	Yes - See Retention Section
Repository Administrator		Originator/Subject Matter Expert	
Chari Fireline - Delivery		William Berry	
File Name			
OMU Aurora Mitigation Plan v10 01-01-18			

<b>Title: Aurora Mitigation Plan</b>	
<b>File Name: OMU Aurora Mitigation Plan v10 01-01-18</b>	
<b>Version: 10</b>	<b>Page: 2 of 12</b>
<b>Effective Date: 1/1/2018</b>	<b>Review Frequency: As Needed</b>

Approvals
<p>Title: <b>Delivery Operations Manager</b></p> <p> _____</p>
<p>Title: <b>Director of Delivery</b></p> <p> _____</p>

<b>Title: Aurora Mitigation Plan</b>	
<b>File Name: OMU Aurora Mitigation Plan v10 01-01-18</b>	
<b>Version: 10</b>	<b>Page: 3 of 12</b>
<b>Effective Date: 1/1/2018</b>	<b>Review Frequency: As Needed</b>

## **1. OVERVIEW**

On October 13, 2010, NERC issued an alert regarding AURORA. This alert replaced the initial distribution of the ES-ISAC Advisory dated June 21, 2007 on AURORA. This document describes OMU's efforts to address vulnerabilities and to mitigate the AURORA threat. This document is considered confidential and should not be distributed outside of OMU unless required by NERC, SERC, or other regulators. A public overview of AURORA can be found in appendix A.

## **2. PROJECT TEAM**

Owensboro Municipal Utilities (OMU) assembled a team to assess AURORA susceptibility and/or develop AURORA mitigation recommendations. The team consisted of the following:

Tim Lyons, Director of Delivery  
Bill Berry, T&D Operations System Supervisor  
Barry Hardy, Delivery Operations Manager  
Austin McLimore, Delivery Engineering Manager  
Russ Evans, Production Technical Services Manager-ESS  
Joanne Stephens, System Support Specialist  
Production Plant Personnel  
Delivery Control Center Personnel

## **3. CUSTOMER INQUIRIES**

As OMU receives customer inquiries regarding AURORA, OMU will first respond by providing the unclassified AURORA Overview document issued by the Department of Defense for public distribution. This document is attached as Appendix A. If desired, OMU will meet privately with concerned customers to discuss the potential impact of AURORA.

## **4. EVALUATION/ASSESSMENT OVERVIEW**

The purpose of this report is to document the OMU efforts to evaluate, assess, and implement mitigation measures to address vulnerabilities related to AURORA. The ultimate intent is to help ensure the reliability of the bulk power system. The specific focus is to protect OMU equipment against AURORA as both a provider of electric power and as a consumer of power.

## **5. PROTECTION & CONTROL ENGINEERING PRACTICES**

OMU utilizes Digital Protection and Control Devices (DPCD) on its transmission system. This includes microprocessor relays and remote terminal devices (RTUs). An evaluation/assessment and description of both of these types of devices is included below.

<b>Title: Aurora Mitigation Plan</b>	
<b>File Name: OMU Aurora Mitigation Plan v10 01-01-18</b>	
<b>Version: 10</b>	<b>Page: 4 of 12</b>
<b>Effective Date: 1/1/2018</b>	<b>Review Frequency: As Needed</b>

### MICROPROCESSOR RELAYS

OMU Delivery and Elmer Smith Station (ESS) Production departments maintain a list of all microprocessor relays used on OMU's transmission system. This list will be reviewed as part of the CIP-002 review process.

In addition, all OMU transmission elements employ sync-check devices to ensure synchronism prior to the closing of transmission facilities. These sync-check devices cannot be accessed or disabled remotely. Consequently, OMU owned microprocessor relays are not expected to impact any high-value electrical rotating equipment.

Since no high-value electric rotating machines are at risk, no additional security measures are required for these devices at this time. However, as electromechanical protection and control devices are replaced with DCPDs, security measures for DCPDs will be reviewed and enhanced as necessary to protect generation and transmission systems.

### RTUs

No high-value rotating equipment security risk is associated with these RTUs.

No additional protection system security measures have been identified as necessary due to AURORA.

## **6. ELECTRONIC AND PHYSICAL SECURITY MITIGATION MEASURES**

Evaluations/assessments of both physical and electronic security have been completed. The results are described below.

### PHYSICAL SECURITY

OMU generating units are connected to the ESS switchyard located on the ESS plant property. To gain physical access to the ESS switchyard, an individual must check-in with a guard at a gatehouse. In addition, the ESS switchyard and all OMU operated substations are fenced with locked gates. The control buildings at the ESS switchyard and all OMU operated substations are locked.

The OMU Delivery Center (which contains the primary control center and primary SCADA servers) and the OMU Cavin Water Plant (which contains the back-up control center and backup SCADA servers) are locked at all times requiring key cards for entry.

No additional physical security measures have been identified as necessary due to AURORA.

<b>Title: Aurora Mitigation Plan</b>	
<b>File Name: OMU Aurora Mitigation Plan v10 01-01-18</b>	
<b>Version: 10</b>	<b>Page: 5 of 12</b>
<b>Effective Date: 1/1/2018</b>	<b>Review Frequency: As Needed</b>

## ELECTRONIC SECURITY

OMU utilized its CIP-002 assessment methodology to identify and evaluate the value and vulnerability of its cyber assets. Electronic access points to OMU's SCADA system and ESS cyber assets are secured behind firewalls. Log-in requires authentication and is monitored.

No additional electronic security measures have been identified as necessary due to AURORA.

## **7. ONGOING MITIGATION EFFORTS**

No additional mitigation efforts have been identified as necessary due to AURORA. OMU will continue to review AURORA documentation and NERC recommendations as they become available to determine if additional actions will be necessary in the future. This mitigation plan will be reviewed annually within 90 days of January 1.

## **8. DOCUMENT APPROVAL TASK LIST**

<b>Document Task List</b>	
1.	Review the Aurora Mitigation Plan and update if necessary.
2.	Verify that the unclassified Aurora Overview document is posted to OMU's website.
3.	File approved Aurora Mitigation Plan in the T&D Operations System Supervisor's office.

## **9. REVISION HISTORY**

<b>Review &amp; Revision History</b>		
<b>Version</b>	<b>Effective Date</b>	<b>Action</b>
5	01-15-2013	Added cover pages. Annual review and approval.
6	01-01-2014	Annual review and approval.
7	01-01-2015	Annual review and approval. Changed "T&D" to "Delivery". Updated titles.
8	01-01-2016	Annual review.
9	12-01-2016	Annual review.
10	01-01-2018	Annual review. Removed statement indicating that OMU SCADA and communication networks are separate and operated independently. Changed review frequency to "As Needed".

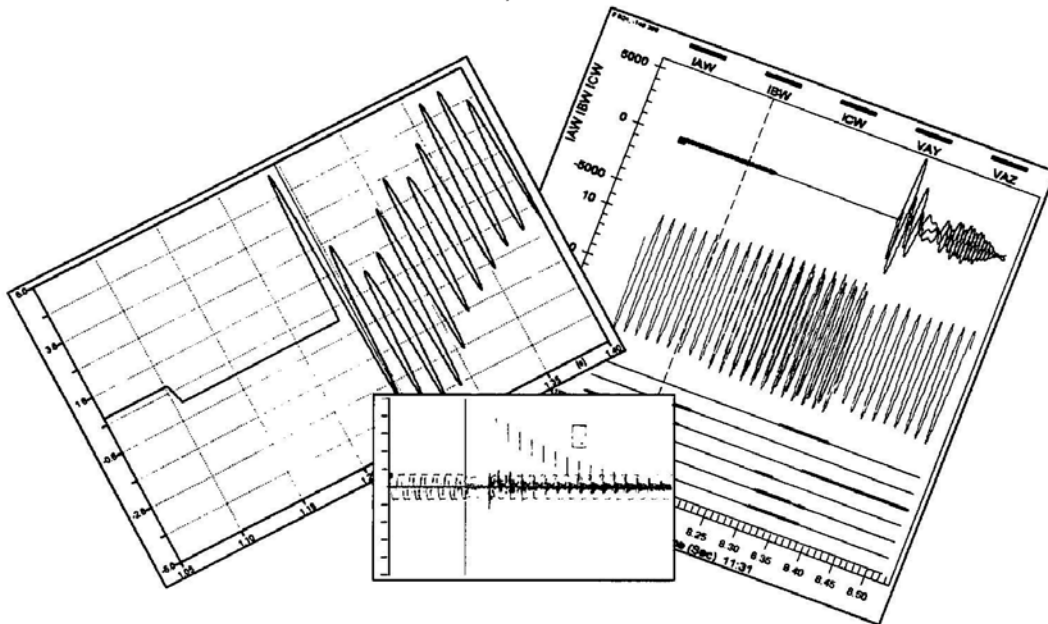
Title: Aurora Mitigation Plan	
File Name: OMU Aurora Mitigation Plan v10 01-01-18	
Version: 10	Page: 6 of 12
Effective Date: 1/1/2018	Review Frequency: As Needed

## Appendix A:

# AURORA Overview document provided by the Department of Defense

UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION

TL Document: O v1.0



# AURORA

## OVERVIEW

Provided Courtesy of DOD

November 2009

**DISTRIBUTION STATEMENT**  
UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION

UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION

**CONFIDENTIAL**

**Local people.**



**Local service.**

Title: Aurora Mitigation Plan	
File Name: OMU Aurora Mitigation Plan v10 01-01-18	
Version: 10	Page: 7 of 12
Effective Date: 1/1/2018	Review Frequency: As Needed

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

**NOTE:** *This document is not an endorsement of any manufacturer or their products. That there is only one Hardware Mitigation Device (HMD) currently available is a simple statement of fact. Again, all other vendors are encouraged to develop similar secure devices to create a larger and more diverse supply.*

**DISCLAIMER**

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

**CONFIDENTIAL**



Title: Aurora Mitigation Plan	
File Name: OMU Aurora Mitigation Plan v10 01-01-18	
Version: 10	Page: 8 of 12
Effective Date: 1/1/2018	Review Frequency: As Needed

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

## **Contents**

1.	AURORA OVERVIEW.....	4
2.	AURORA: MYTHS VS. FACTS .....	5

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

**CONFIDENTIAL**



<b>Title: Aurora Mitigation Plan</b>	
<b>File Name: OMU Aurora Mitigation Plan v10 01-01-18</b>	
<b>Version: 10</b>	<b>Page: 9 of 12</b>
<b>Effective Date: 1/1/2018</b>	<b>Review Frequency: As Needed</b>

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

## **OVERVIEW**

### **1. AURORA OVERVIEW**

The safe and reliable supply of electric power is vital to national security and economic and social stability. A significant, cross-sector vulnerability exists in the Nation's power grid that jeopardizes the availability and safety of electric power and the safety and reliability of many types of motors and generators connected to it. The vulnerability, dubbed AURORA, is a text book example of just one in a growing number of unintended consequences we are facing as a direct result of modern advances in materials and digital technology. The trend is further compounded by our continued failure to thoroughly consider and address lifecycle security issues before deploying new technology. As such, we are inadvertently creating new and asymmetric opportunities to damage or disrupt critical assets while widening the gaps in our ability to protect them. Although originally socialized as a cyber security issue, AURORA actually describes a narrow, but significant and exploitable gap in electrical protection that exists in the power grids of many countries.

AURORA is neither theoretical nor an academic topic. The fundamental principles behind it are actually quite simple and well understood by experienced and practicing utility engineers and operators. Rotating equipment such as motors and generators spin in sync with the power grid. Utilities have known for years that if rotating equipment is brought onto or reconnected to the grid out of sync, or "out of phase," damaging shaft and winding torques will result as the machine is instantaneously forced back into synchronization by the power of the Grid. Basic laws of physics govern the consequences and the resulting torque can easily exceed mechanical design limits, damaging or destroying rotating equipment as well as their connected loads, e.g., pumps and gear boxes. Over the years, the likelihood of damage from out-of-synchronization events led to the development and refinement of complex protection and control schemes specifically designed to prevent them. Yet, historical incidents of accidental malfunction and maloperation have proved that the risk of damage from inadvertent reclosures is real and persistent. This risk will likely continue as the use of high-speed breakers; complex, multi-featured, intelligent end devices and network convergence technologies continues to grow.

AURORA events can occur accidentally or intentionally. An AURORA "attack" is simply a deliberate attempt to damage or destroy susceptible equipment. Another unique aspect of AURORA is that vulnerable facilities could implement all traditional physical and cyber security best practices to protect their own breakers and electric switchgear from compromise, and still be vulnerable to an attack from outside their fence. One need only gain physical or cyber access to a relevant upstream commercial substation breaker.

In the main, AURORA has been thoroughly modeled, tested, demonstrated, and validated by a qualified team of public and private engineering and security experts. The consequences of AURORA-based damage can impact equipment that is necessary to maintain our quality of life. Large motors and generators are of particular concern because they are expensive and can have repair or replacement lead-times ranging from several months to years. Consequently, the Director of the Defense Critical Infrastructure Program (DCIP), Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (OASD-HD&ASA) established a program to mitigate AURORA in Defense facilities. Their information and research is now being freely shared with other government and private sector entities.

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**  
Page 4 of 7

**CONFIDENTIAL**

Title: Aurora Mitigation Plan	
File Name: OMU Aurora Mitigation Plan v10 01-01-18	
Version: 10	Page: 10 of 12
Effective Date: 1/1/2018	Review Frequency: As Needed

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

A hardware mitigation device (HMD) was developed to serve as an interim mitigation until either a better solution is developed and/or overall Grid physical and cyber security postures mature sufficiently to neutralize the vulnerability. The HMD consists of a purpose-built, commercial protective relay. It contains a patented protective algorithm that has been available to all relay vendors since its licensure; however, to date only one U.S. firm has adopted it in its product line. Its remote access capabilities have been removed at the factory in order to eliminate the possibility of remote compromise. Combined with prudent physical and cyber security measures, the HMD is designed to provide facilities substantial protection against damage from accidental or intentional AURORA events. Enhancing the physical and cyber security postures of supporting electric power providers is another positive action to improve overall effectiveness.

While individual configurations and protection needs will vary, the general guideline for planning purposes is one HMD per incoming utility feeder line; and/or they can be placed directly in front of specific on-site rotating equipment as an added layer of protection against internal mishaps or compromises. However, in all cases, they must be installed on switchgear inside the facility's security perimeter where positive physical control of the device can be maintained. Once installed, the HMDs continuously monitor the status of the incoming power. If they detect the beginning of an AURORA event, whether intentional or accidental, they are designed to immediately open the facility's breaker in time to prevent damage to its downstream equipment. The operation of the HMD has been thoroughly tested and 3<sup>rd</sup> party-validated. In all qualified trials and testing, the HMD performed exactly as designed. It actuates on AURORA events only and leaves all other conventional power transients and faults to normal system protections.

The HMD installation process is relatively straightforward. Relevant electrical drawings, studies, and equipment specifications are gathered, analyzed and if necessary, modeled by the particular facility. If a vulnerable facility contains susceptible rotating equipment that warrants protection, then further analysis is conducted to determine optimum number, placement, and settings for actual HMD installations. Depending on local labor rates and economy of scale, typical relay installations should run approximately five times the cost of each installed relay. While installation of the HMDs may be straightforward, gaining senior level buy-in and support has been a persistent challenge.

## **2. AURORA: MYTHS VS. FACTS**

During AURORA's initial discovery and validation in 2007, the issue attained extremely high visibility, which eventually led to interest from the National Security and the Homeland Security Advisors to the President. As the initial round of briefings moved up various federal organizational charts, they were taken out of the hands of technical personnel thoroughly versed in the subject and presented by non-technical staffers who were not. In these subsequent briefings, many of the salient facts of AURORA were misinterpreted or simply lost. Absent accurate and timely briefings, bad information became fact, and fact became myth. At some senior government levels AURORA has been incorrectly briefed as a computer virus; other ranking officials have been told that a simple software patch will fix the problem. As a result, decision makers have been denied a fair opportunity to make accurate and responsible risk management decisions based on fact. Instead they were unknowingly acting on inaccurate information from what they had perceived to be authoritative sources. Listed below are some of the more persistent myths surrounding AURORA.

**MYTH:** The AURORA generator test was staged and controls and protections had been removed or otherwise disabled in order to achieve the "desired" results.





Title: Aurora Mitigation Plan	
File Name: OMU Aurora Mitigation Plan v10 01-01-18	
Version: 10	Page: 11 of 12
Effective Date: 1/1/2018	Review Frequency: As Needed

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

**FACT:** All normal and expected system and Grid protections were fully enabled and operational. The configuration was checked and validated by independent, disinterested third party experts whose combined industry experience measured in the hundreds of years. A fundamental ground rule of the demonstration was that if ANY system protection actuated to prevent the attack, the test would be aborted immediately. The only condition that was assumed for the test was gaining remote access into the system. Previous works had already demonstrated the ease at which remote access could be achieved and the objective of the test was to demonstrate that conventional protection schemes could not react in time to prevent equipment damage from AURORA.

**MYTH:** AURORA will be mitigated once utilities implement NERC's CIP Standards.

**FACT:** The CIP Standards only apply to certain bulk electric system assets; Distribution assets, from which most military and industrial facilities receive their electric power, are not subject to CIP requirements.

**MYTH:** A simple software patch exists to "fix" AURORA.

**FACT:** No, there is no patch, nor is AURORA a patching issue. True protection should be implemented inside the fence line of the facility with the equipment that can be damaged. A simple view is the Power Grid is the weapon, and not affected, the load or customer is the target.

**MYTH:** Utilities can modify their current protection schemes or relay configurations to protect their customers against an AURORA event and still maintain today's efficiency and reliability.

**FACT:** While this proposition may sound appealing on its face, the root of AURORA is the very gap between the ability to cause damage and the inability of conventional protection schemes to prevent it and still maintain stability. The delivery of electric power has been finely tuned over the years to provide a purposeful and effective balance between protection and reliability. In simplistic terms, the complex coordination and protection schemes of the modern day grids are configured *tight* enough to prevent most damage from inadvertent mishaps, but *loose* enough to prevent false trips and nuisance outages. The manpower and financial resources necessary to attempt such a large scale reconfiguration, let alone the risk involved in major configuration changes, soon renders this option impractical. Secondly, the ease at which unauthorized remote access can be had would likely negate the modified configurations because the attacker could simply change them back. Finally, we are entering a new age of asymmetric threats and consequences in critical infrastructures such that end customers and asset owners may no longer wish to rely solely on their utility for protection. Given today's hostile Internet environment, most companies (and individuals) do not rely solely on their ISP for protection, but add additional layers of protection against hackers and other Internet-based threats.

**MYTH:** Only motors greater than 800hp need be considered for mitigation.

**FACT:** While smaller motors may be cheaper, easier to replace, and more likely to withstand a single hit from an AURORA event than large motors, the decision to mitigate should not be based on equipment size. Instead, a simple three-part analysis can be used to reach a more responsible risk management decision: 1) is the equipment (motors and their connected loads) susceptible to AURORA? If so, then 2) considering all costs associated with their loss or damage, are they worth protecting? If so, then 3) is the commercial power supply strong enough cause damage during an AURORA event? If the answer to all three is yes, then mitigate the risk.

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

Page 6 of 7

**CONFIDENTIAL**

Title: Aurora Mitigation Plan	
File Name: OMU Aurora Mitigation Plan v10 01-01-18	
Version: 10	Page: 12 of 12
Effective Date: 1/1/2018	Review Frequency: As Needed

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

**MYTH:** The actual “generator” of the AURORA test generator was not damaged during the test.

**FACT:** Post-test forensics examination determined that not only was the generator’s diesel engine destroyed, the winding on one phase of the generator were reduced to 30% of rated capability, damaged beyond use. The \$400,000 generator was sold for scrap and considered beyond repair.

**MYTH:** The entire test was staged to the extent that pyrotechnics were used to simulate the destruction of the generator.

**FACT:** Unfortunately, this is one of the more sensational myths associated with AURORA. Actually, the white smoke observed in the video was due to catastrophic failure of the large rubber coupler/dampener joining the prime mover (diesel engine) to the generator shaft. The black smoke was from engine damage and eventual destruction.

In conclusion, AURORA has been aired on global news programs, blogged on the Internet, and discussed at public conferences to include hacking conferences. Given its simplicity and international exposure, it would be remiss to assume that our adversaries were not already thoroughly versed in the phenomenology and practical application of AURORA. Actions are underway to provide utility and industrial sectors with all of the technical facts and engineering data necessary to assess and mitigate their risk from what will one day prove to be just another in a long list of new asymmetric, technological attack vectors.

**UNCLASSIFIED  
FOR PUBLIC DISTRIBUTION**

Page 7 of 7

**CONFIDENTIAL**