

APRIL 9, 2026 | NEPOOL PARTICIPANTS COMMITTEE

# nGem and Cyber Security Updates

---



Rudy Pawul

VICE PRESIDENT, INFORMATION AND CYBER SECURITY SERVICES



# nGEM Background

- ISO-NE markets use GE Vernova's suite of market applications
- nGEM is a modernization effort (Next Generation Markets) incorporating new technologies and standardizing its code set among multiple ISOs
  - ISO-NE, PJM, and MISO participated, sharing development costs for the base product

# nGEM Program Goals

## Incremental Upgrade

Incrementally replace current market system to reduce risk to Operations

## Security

Design for industry standard Cyber Security requirements (NERC, IRC/ITC). Proactive approach to CIP compliance

## Standardization

Standardize various ISOs' features into the nGEM product where possible

## High Performance

High performance with flexibility to choose different solvers

## Maintainability

Ensure system stays current and remains a product. Support faster market rule implementations

## Test Automation

Allow each new release to be regression-tested against existing system

# Technology Modernization

- “DevOps” methodology for a continuous delivery approach that enables more frequent delivery of:
  - **Defect** fixes
  - **Security** patches
  - **Third-party software** updates
- Utilizes a “Containerized” (Kubernetes) environment
  - Provides improved **scalability, resiliency, and flexibility** for all market systems
- Introduces data streaming (Kafka)
  - Enables higher-fidelity, lower-latency data exchange across the system
  - Eliminates reliance on file transfers between market system components
- **Automated test framework** becomes a “living” library of all MCE functions

# What are containers?

- Containers are a way to isolate applications running on the same machine from one another
  - This allows multiple applications to run on the same resources without problems due to shared dependencies



- Analogous to using containers to allow you to fit more food (applications) in your refrigerator (server) without the contents (dependencies) co-mingling
- Similar to how VMware virtualizes servers to reduce the amount of hardware in the data center, containers virtualize applications to reduce the number of servers

# Improved Monitoring and Observability

- Modern monitoring tools built into containers to enable deeper visibility into clearing engine behavior:
  - **Splunk** logging
  - **Grafana** dashboards
  - **Jaeger** tracing
  - **Prometheus** event monitoring
- Dynatrace observability feeds OpsGenie automatic callouts to support personnel on a macro level
- These tools improve **situational awareness** for IT and Infrastructure teams

# Real-Time Market Clearing Engine

- Consolidates day ahead and real time study modes into one unified Market Clearing Engine (MCE)
- Improved performance for faster solution times
  - Allows for more accurate physical modeling for complex resources
- 2026 – Implement Real-Time Unit Commitment and Coordinated Transaction Scheduling and Pricing Engine
- 2028 – Implement Unit Dispatch, Contingency and other remaining modes and retire legacy systems

# CYBERSECURITY HIGHLIGHTS



# 2025 Project Highlights

- Further bifurcation of observability tools
  - Created enterprise-only Security Information and Event Management and Network Detection and Response tool installations
  - Allows for isolating operational technology environment, while still having observability
- Refinements to phishing testing
- Earlier integration of Application Security Testing
  - Identifies code and configuration security flaws as part of the development process to avoid slowing developers down
- Expansion of “immutable” backups to cloud resources

# 2026 Project Highlights

- Electronic Security Perimeter redesign for increased resiliency, isolation between control centers, zero-trust, and easier demonstration of CIP compliance
- Additional network projects to ensure post-quantum computing readiness
- Moving from Vulnerability Management to Continuous Threat Exposure Management

# Security Operations Center Action Highlights due to the War with Iran

- Built and updated the operational threat picture
  - Refined the integrated cyber/kinetic assessment of the Iran situation (e.g. no credible intelligence indicating that Russia or China are providing cyber assistance to Iran)
- Tactics and techniques coverage review
  - Compared current security controls to known adversary methods
- Reviewed and validated all monitoring and protection tools
- Processed cyber threat intelligence
  - Reviewed cyber threat indicators received from federal partners
  - Searched across ISO environments to confirm no matches with known malicious indicators
- Monitored for identity-based attacks
  - Created additional searches to detect “MFA fatigue”
- Delivered cyber risk posture briefings to ISO Control Room and Local Control Center leadership teams

# Questions

