

U.S. Nuclear Regulatory Commission  
38<sup>th</sup> Annual Regulatory Information Conference

# RIC2026

Regulation, Innovation and  
Collaboration for a Safer Tomorrow

March 10-12, 2026

Bethesda North Marriott Hotel  
and Conference Center  
Rockville, MD

#NRCRIC2026

NRC.gov



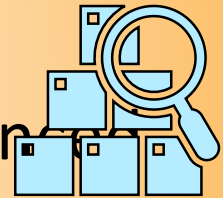
# Cybersecurity Enhancements

Office of Nuclear Security and Incident Response

## Overview

# Modifications of cybersecurity to address the ADVANCE Act and EO 14300 5(g) (Reforming and Modernizing the NRC's Regulations)

- New/Revised Cybersecurity Inspection Procedures
  - Enhance clarity and effectiveness
  - Enable the future: nuclear plant restarts and advanced reactor technologies
- Research to Prepare for the Future
  - Ensure safety and security as technology evolves



## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - Restarts
  - Construction
- Preparing for the Future
  - Zero-Trust Architecture
  - Cloud Computing
  - Artificial Intelligence (AI)
  - Autonomous Operations

# Risk-informing Operating Fleet Inspections



Goal: Incorporate lessons learned and balance the level of resources with safety significance.

- Biennial -> Triennial inspection cycle
- Streamlined Information Gathering Process
- Incorporated Risk Informed & Consequence-based guidance to aid CDA selection

## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - **Restarts**
  - Construction
- Preparing for the Future
  - Zero-Trust Architecture
  - Cloud Computing
  - Artificial Intelligence (AI)
  - Autonomous Operations

# Enabling Safe, Efficient Plant Restarts

Goal: Ensure nuclear facilities reestablishing operating licenses have implemented cybersecurity programs that meet regulatory requirements.

- One-time -> Pre-fuel and post-fuel inspections
- Information Gathering Process aligned with Operating Fleet
- Incorporated Risk Informed & Consequence-based guidance to aid CDA selection

## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - Restarts
  - **Construction**
- Preparing for the Future
  - Zero-Trust Architecture
  - Cloud Computing
  - Artificial Intelligence (AI)
  - Autonomous Operations

# Supporting the Inspections of New Reactors



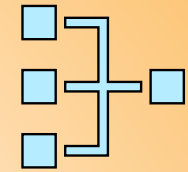
Goal: For diverse reactor designs and novel cyber technologies, including those for **advanced reactors** and **small modular reactors**, staff plan to verify the implementation of cybersecurity program requirements by:

- One-time -> Pre-fuel and post-fuel inspections
- Critical systems for inspection will be identified
- Using Information Gathering Process aligned with Operating Fleet

## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - Restarts
  - Construction
- Preparing for the Future
  - Zero-Trust Architecture
  - Cloud Computing
  - Artificial Intelligence (AI)
  - Autonomous Operations

# Zero-Trust Architecture (ZTA)



Reactors may adopt technologies such as remote access and autonomous operations that could jeopardize the current perimeter-based cybersecurity architecture. ZTA is a new paradigm that moves security from perimeter defense to focus on users, assets, and resources.

NRC staff have published research on how ZTA could be implemented in nuclear facilities.

## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - Restarts
  - Construction
- Preparing for the Future
  - Zero-Trust Architecture
  - **Cloud Computing**
  - Artificial Intelligence (AI)
  - Autonomous Operations

## Cloud Computing

Nuclear facilities may wish to use cloud services to manage critical digital assets and data across locations.

NRC staff are conducting research on how cloud-based technology could be safely and securely implemented to mitigate the potential increased risk of third-party vulnerabilities. Research will potentially be used to inform future guidance.

## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - Restarts
  - Construction
- Preparing for the Future
  - Zero-Trust Architecture
  - Cloud Computing
  - Artificial Intelligence (AI)
  - Autonomous Operations

## Artificial Intelligence (AI)



The nuclear industry has expressed a growing interest in using AI to improve operational performance and mitigate operational risk.

NRC staff have published research on how AI and machine learning could be used to assist in cybersecurity event analysis.

NRC staff are researching additional benefits and risks of AI as part of the cybersecurity infrastructure.

## Topics

- Cybersecurity Inspections
  - Operating Fleet
  - Restarts
  - Construction
- Preparing for the Future
  - Zero-Trust Architecture
  - Cloud Computing
  - Artificial Intelligence (AI)
  - **Autonomous Operations**

## Autonomous Operations

Future reactors may use autonomous systems to perform tasks without direct human control, potentially reducing staffing costs.

NRC staff have published research on a potential framework to characterize autonomous systems. NRC staff are continuing to conduct broader evaluations and research on the operational and cybersecurity risks associated with the use of autonomous systems.

## Inspection Procedures

See QR code for links to the Inspection Procedures.

Cyber IPs include:

- IP 71130.10 – Operating Fleet
- IP 81000.12 – Pre-Fuel Load Restart
- IP 81000.13 – Post-Fuel Load Restart
- IP 75100.09 – Pre-Fuel Construction (Future)
- IP 75100.15 – Post-Fuel Load Construction (Future)



## Contacts

This presentation was made by staff in the Cyber Security Branch (CSB).

Jim Beardsley, Chief  
NSIR/DPCP/CSB  
[Jim.Beardsley@nrc.gov](mailto:Jim.Beardsley@nrc.gov)

Rodney Fanner  
Reactor Systems Engineer  
[Rodney.Fanner@nrc.gov](mailto:Rodney.Fanner@nrc.gov)

Tanvir Siddiky  
Reactor Systems Engineer  
[Tanvir.Siddiky@nrc.gov](mailto:Tanvir.Siddiky@nrc.gov)

Priscilla Wu  
IT Specialist (Cyber)  
[Priscilla.Wu@nrc.gov](mailto:Priscilla.Wu@nrc.gov)

## Ongoing and future research

See QR code on the right for links to the Research topics:

- Zero-Trust Architecture
- Cloud Computing
- Artificial Intelligence (AI)
- Autonomous Operations



## Contacts

This presentation was made by staff in the Cyber Security Branch (CSB).

Jim Beardsley, Chief  
NSIR/DPCP/CSB  
[Jim.Beardsley@nrc.gov](mailto:Jim.Beardsley@nrc.gov)

Rodney Fanner  
Reactor Systems Engineer  
[Rodney.Fanner@nrc.gov](mailto:Rodney.Fanner@nrc.gov)

Tanvir Siddiky  
Reactor Systems Engineer  
[Tanvir.Siddiky@nrc.gov](mailto:Tanvir.Siddiky@nrc.gov)

Priscilla Wu  
IT Specialist (Cyber)  
[Priscilla.Wu@nrc.gov](mailto:Priscilla.Wu@nrc.gov)