Facility Ratings Activities

Steven Noess, Director, Regulatory Programs, NERC
Teresina Stasko, Assistant General Counsel and Director of Enforcement, NERC
Tim Ponseti, VP Operations, SERC
Tom Galloway, CEO, NATF
February 9, 2022

RELIABILITY | RESILIENCE | SECURITY

PREVENTATIVE

- Outreach and Education around Risk
  - ERO Enterprise CMEP Practice Guide (published Q2 2020)
  - Workshops
  - Newsletters
- Engage with industry
- Examine current Standard for potential adjustments

ASSESSMENT

- Current conditions
- Recent monitoring

RECOVERY

- Sharing practices
- Enhanced mitigation activities

RELIABILITY | RESILIENCE | SECURITY

Relay Loadability

Operations

Modeling /Analysis

Facility Ratings

Operations Planning

Data Specification

Planning
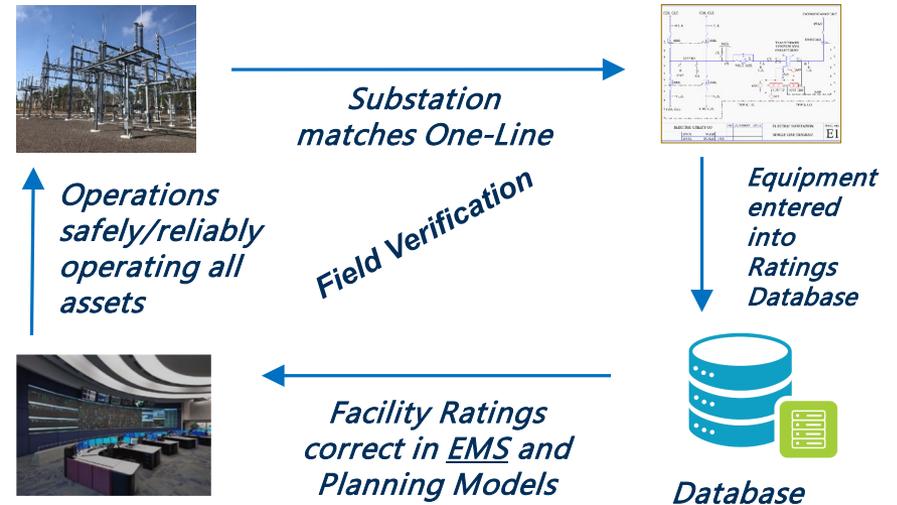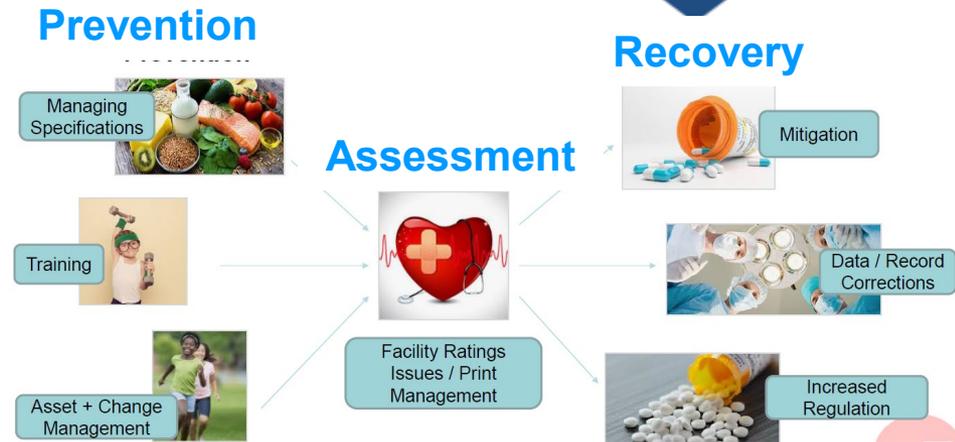
- Support development and sustainment of registered entity risk-based Facility Ratings programs and resolution of Facility Ratings noncompliance using existing tools

  - Key Themes / Fall-downs

  - Risk based approach

- Registered entities should develop or continue approaches for self-assessment and risk-based prioritization

  - Align compliance with operations

  - Report and mitigate
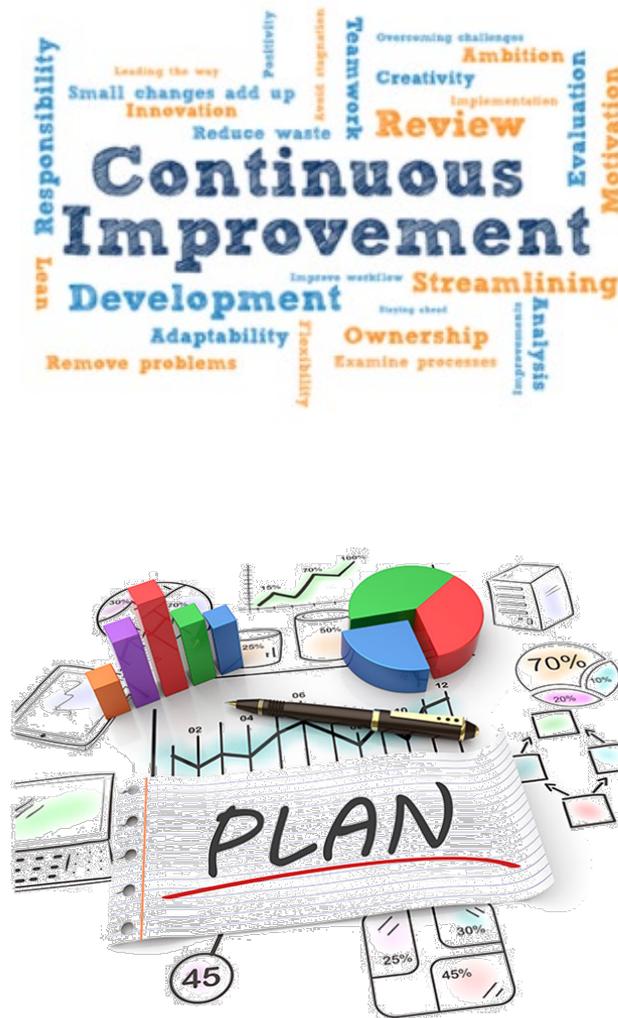
- Identify a facility ratings **sponsor and owner**

- Establish **clarity on the foundational components** of the facility ratings process or program

- **Manage data** to ensure accuracy

- Establish an **accurate baseline** to determine accuracy of facility ratings

- Establish **comprehensive work practices** for planned construction, acquired facilities, and unplanned or restoration work

- Validate through **periodic reviews**

- Implement **human performance measures**

Internal Controls – embedded throughout the practice areas

Incorporation of these elements facilitates sustainability of the program/processes

About 50 practices overall, some with "sub-practices"

Not Implemented
(Absent - the practice is not performed in the organization)

Partially Implemented
(Incomplete, with multiple opportunities for improvement)

Largely Implemented
(Complete, with a recognized opportunity for improvement)

Fully Implemented
(Complete)

Reporting %

- 90% → 93% → 94% % NATF T-mileage
- 85% → 93% % NATF Membership
- 80% → 83% → 84% %NA T-mileage (>100kV)

FALL-2020 · SPRING-2021 · FALL-2021

High Participation with continued increase!

Upward trend across all practices!

Focus Areas

Category	Current Score		Score Trend		
Overall	72%		66%	68%	72%
Internal Controls	70%		64%	67%	70%
Sponsor and owner	80%		73%	76%	80%
Foundational program components	79%		72%	76%	79%
Data accuracy	76%		73%	75%	76%
Establish baseline	61%		55%	56%	61%
Establish work practices	70%		64%	66%	70%
Periodic reviews	54%		45%	46%	55%
Training/HP measures	68%		62%	64%	68%

RELIABILITY | RESILIENCE | SECURITY

ERO Enterprise CMEP Facility Ratings Interactions by Inherent Risk 2017 – 2021

TO Function Entities that had an Engagement/ Monitoring from 2017-2021

GO Function Entities that had an Engagement/ Monitoring from 2017-2021
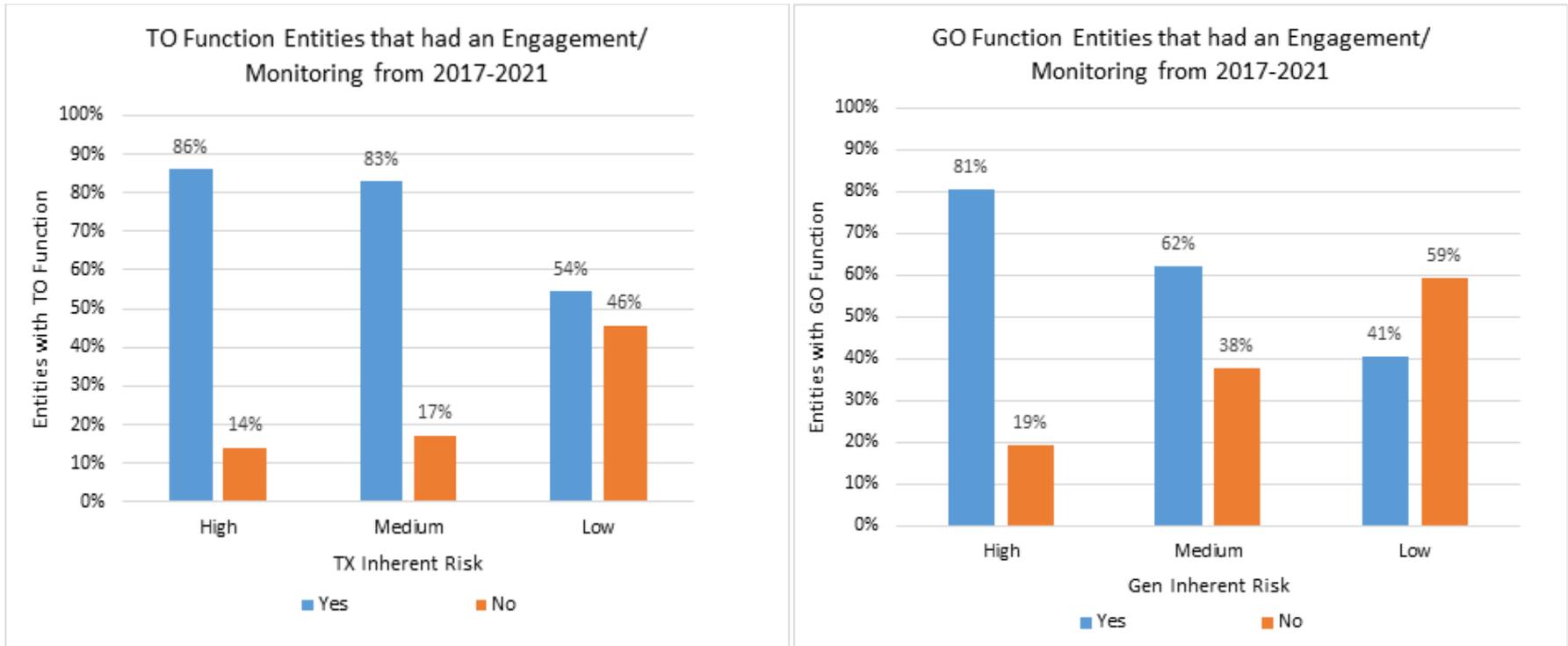
- Next steps
  - Continued use of risk-based approach
    - Monitoring activity for entities that have not had a CMEP activity related to Facility Ratings since 2017
    - Continued emphasis of FAC-008 in planned 2022 compliance monitoring activities (CMEP Implementation Plan)
    - Enforcement dispositions based on risk to BES
  - Continued outreach
  - Alignment of priority with stakeholders and regulators

Questions and Answers

RELIABILITY | RESILIENCE | SECURITY

- Compliance Guidance Timeline

- Compliance Guidance Policy

- Implementation Guidance

- CMEP Practice Guides

- Historically Many Compliance Documents
  - Compliance Application Notices (CANs), Compliance Analysis Reports (CARs), Bulletins, Technical Rationale, etc.
- Distinct from Reliability Guidelines, etc.
- Desire to Consolidate
- Compliance Guidance Review Team
- 2015 NERC BOT Approved Compliance Guidance Policy
- Supporting Tools and Resources Developed

Compliance Guidance Policy (CG)

CMEP Practice Guides (PG)

Implementation Guidance (IG)

Compliance Guidance

1st CMEP PG: Deference To IG

BOT Approved CG Policy

Previous Guidance Reviewed & Retired (CANs, Directives, Etc.)

Enhancements Identified & Tools Developed

CG Website Enhanced

Periodic Review Process Required for New IG

PG Clarifying Header

2015	2016	2017	2018	2019	2020	2021	2022

CG Procedures Developed & Implemented

Webinar:CG Best Practices & Lessons Learned

CG Enhancement Surveys

Webinar: CG Enhancements & Tools

SDT Instruction

Periodic Review on Endorsed IG

Webinar: CG Process, Best Practices, Tools, and Resources (Planned)

- Examples or Approaches
  - How to "Implement" Reliability Standards
- Reliability Standard or Topic Specific
- Developed <u>by</u> Industry <u>for</u> Industry
  - Pre-Qualified Organization (PQO)
  - Standard Drafting Team (SDT)
  - Regional Entity Stakeholder Committees

- Must be "endorsed" by ERO Enterprise
  - Recognizes guidance as appropriate for deference during CMEP activities
  - Agrees entities can rely on the guidance
  - Endorsement is appropriately a high bar
- ERO Independence and Objectivity remains critical
- Publicly posted
- Perceptions:
  - Endorsement is Difficult
  - Endorsement is Time Consuming
  - Storage for GTB/TR

- **Tools & Resources**[*]
  - IG Development and Review Aid
  - IG Template
  - PQO/SDT Contact Information
  - Non-Endorsed IG Tracking
  - IG Under Consideration/Development Spreadsheet
  - Compliance Guidance Webpage
  - One Stop Shop

*Covered During November 2020 CG Webinar

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

- ## Implementation Guidance Development Aid

Color Code Key:
Automatic Non-Endorsement
Increased Likelihood of Non-Endorsement
Multiple Occurrences/Severity of Occurrences could lead to Non-Endorsement

	Implementation Guidance Development Aid	
	Items for Consideration	✓
1.	Ensure IG does not conflict with, or change, the Purpose or Applicability of the Reliability Standard.	
2.	Ensure IG does not conflict with, or change, the meaning or intent of the Requirement and Measure.	
3.	Ensure IG does not include language that attempts to describe an audit approach.	
4.	Ensure IG does not conflict with, or contradict, FERC or ERO Enterprise documents such as FERC Orders, FERC Interpretations, Reliability Standard Audit Worksheets (RSAW), Endorsed Implementation Guidance, Compliance Bulletins and Directives, Reliability Standard Implementation Plans, Reliability Standard Guidelines and Technical Basis, NERC Glossary of Terms, etc.	
5.	Ensure IG does not make the Reliability Standard and Requirement less restrictive.	
6.	Ensure IG does not lead the entity to believe there are additional compliance obligations that are not specifically required by the subject Reliability Standard and Requirement.	
7.	Ensure IG does not skip steps or stop short of complying, and addresses the entire Requirement in sufficient detail.	
8.	Ensure IG provides specific examples or approaches to compliance.	
9.	Ensure IG is not a whitepaper, position paper, concept paper, FAQ, or technical reference document.	
10.	Ensure the body of the IG document only includes specific examples or approaches to compliance and does not include supporting/reference information that should be housed in the Appendices. NOTE: Appendices could include templates, theory, calculations, models, tables, drawings, graphics, good practices, definitions, terminology, glossary, white papers, FERC orders, Guideline and Technical Basis, Technical Rationale, IG authors, etc.	
11.	Ensure IG is not region specific, such as guidance for a Regional Reliability Standard.	
12.	Ensure IG includes a plan for PQO/SDT periodic reviews and updates to ensure guidance remains current and valid. Reviews should include elements such as updates or revisions to items such as FERC Orders, FERC Interpretations, Reliability Standard	

- [Frequently Asked Questions](#)

Compliance Guidance Frequently Asked Questions (FAQ) — NERC document, December 2020, with Q&A content on Compliance Guidance - General.

- Tracking of [Non-Endorsed Implementation Guidance](#)

  ▪ Provides reasons for non-endorsement (consistent with Development Aid reasons)

	Non-Endorsed Implementation Guidance - Last Updated 1/5/2022		
Year	**Implementation Guidance Title**	**Additional Information**	**Date Announced**
2021	CIP-005-7 R3 Electronic Security Perimeters (2019-03 SDT)	Pending - Check Back Later	1/5/2022
	CIP-010-4 R1 Configuration Change Management and Vulnerability Assessments (2019-03 SDT)	Pending - Check Back Later	1/5/2022
	CIP-013-2 Supply Chain Risk Management Plans (2019-03 SDT)	Pending - Check Back Later	1/5/2022
	CIP-004-7 Personnel & Training (2019-02 SDT)	Pending - Check Back Later	1/5/2022
	EOP-011-2 Emergency Operations and Preparedness (2019-06 SDT)	The ERO Enterprise declined to endorse this Implementation Guidance because it does not provide sepcific examples, or approaches, on how an entity could meet compliance. Additionally, the proposed IG is less stringent than the standard and thus possibly misleading, or subject to misinterpretation.	1/5/2022
	CIP-004-6 and CIP-011-2 Cloud Solutions and Encrypting BCSI (RSTC)	The ERO Enterprise declined to endorse this proposed Implementation Guidance document because it does not address many of the concerns identified in the initial IG review in 2020. Specifically the guidance should be vendor agnostic, or a disclaimer should to be included that states the elements prescribed in the guidance is relevant at the time it is written. It is understood that vendors change their practices and therefore this information in the guidance may become irrelevant later down the line. In the 'Evidence Example' the "notification for terminations" statement is problematic as it does not align with the language of the standard, which is "termination action". Under 'Terms' the "Shared Responsibility Model" needs to be struck, or further clarified, as it implies transference of compliance obligations. Some of the elements in the 'Evidence Example' would fail to demonstrate compliance over the course of time. Overall the guidance can be misleading and needs additional clarity.	8/12/2021
	CIP-007-6 R1 Software Defined Networking: Logical Network Accessible Ports (EnergySec)	The ERO Enterprise unanimously declined to endorse this proposed Implementation Guidance document because it does not provide specific approaches or examples for an entity to demonstrate compliance. Additionally, the proposed Implementation Guidance is written as a whitepaper or a position paper. The proposed document provides no specific compliance implementation guidance. The ERO Enterprise stresses the importance of the use of the Implementation Guidance Development Aid.	8/12/2021
	CIP-005-6 R2.4_R2.5 Vendor Support via Web Conferencing (NATF)	The ERO Enterprise declined to endorse this Implementation Guidance as the proposed NATF IG does not provide examples or approaches for registered entities to comply with CIP-005-6 Requirement R2. Instead, the proposed IG introduces positions and definitions (e.g. vendor remote access and control) which may be viewed as changing the meaning of the requirement or interpreting the requirement. Additionally, the proposed IG contains statements that may be viewed as limiting CMEP personnel's ability to obtain reasonable assurance of compliance. As an example, the proposed IG contains the following statement "there is no compliance evidence to retain for each such session". In summary, the proposed IG did not sufficiently address the Implementation Guidance Development and Review Aid.	4/28/2021
	CIP-013-2 Supply Chain Risk Management Plans (2019-03 SDT)	The ERO Enterprise declined to endorse this Implementation Guidance as several revisions are necessary for clarity purposes in order to avoid entity confusion.	3/24/2021
	CIP-010-4 R1 Configuration Change Management and Vulnerability Assessments (2019-03 SDT)	The ERO Enterprise declined to endorse this Implementation Guidance as several revisions are necessary for clarity purposes in order to avoid entity confusion.	3/24/2021
	CIP-005-7 R3 Electronic Security Perimeters (2019-03 SDT):	The ERO Enterprise declined to endorse this Implementation Guidance as some of the examples provided were incomplete which could lead to entity misinterpretation of the examples. Additionally, there are several misleading statements regarding "staff augmentation". Finally, there are inconsistencies in the use of similar, but different, terminology which could lead to entity confusion.	3/24/2021
	PRC-019-2 Coordination of Voltage Control Systems, Protection Systems, and Equipment Capabilities (RSTC)	The ERO Enterprise unanimously declined to endorse this document for the reasons that follow. The IG conflicts with line 15 of the Implementation Guidance Development and Review Aid, which states IG shouldn't be a whitepaper or technical reference. The calculations should be more of an appendix. The example should be more what things are considered and how, calculations are not the thrust of that. Additionally, none of the examples speak to the plant control system for dispersed power producing resources. Finally, Table 3.1 mentions using the Unsaturated Transient Reactance when evaluating Loss of Field (40) settings for PRC-019-2 compliance, which is apparently an error which disagrees with the calculations in the appendix of IEEE Standard C37.102-2006, which is an Associated Document of PRC-019-2 which uses Saturated Transient Reactance.	12/8/2020

- Does Not Include Examples or Approaches

- Changes Scope of Requirement

- Includes Incomplete/Misleading Examples

- Includes Interpretation/Position Statement

- Whitepaper, Technical Reference, etc., that does not meet criteria

- 19 active ERO Enterprise-Endorsed (10 CIP, 9 O&P)*
  - NATF: 5
  - MRO Standards Committee (MRO SC): 4
  - Operating Committee (OC): 3
  - Planning Committee (PC): 2
  - Critical Infrastructure Protection Committee (CIPC): 2
  - CIP Standard Drafting Teams (SDTs): 2
  - MRO CMEP Advisory Council (MRO CMEPAC): 1

  *As of January 25, 2022

RELIABILITY | RESILIENCE | SECURITY

- Industry Webinar
  - Address Current Issues
  - Focus on IG Development
  - Discuss Best Practice
  - Encourage Use of Available Tools and Resources
- Coordinate alternatives with SDTs for non-IG material
- Work with Pre-qualified organizations that seek interim collaboration

- Guidance for ERO Enterprise staff

- Serves ERO Enterprise interest to support consistency of approach

- Developed <u>by</u> ERO Enterprise <u>for</u> ERO Enterprise

- Publicly posted solely for transparency

- ERO Enterprise development practices:
  - Track as part of "Program Alignment Process"
  - Seek Compliance and Certification Committee (CCC) input to confirm intent/perspective

- PGs are not compliance approaches
- PGs do not change or supersede any standard
- Developed to support ERO Enterprise Independence and Objectivity
- CMEP activities broader than "compliance"
  - Understanding how entities mitigate risk
  - Performance and internal controls
  - Inform oversight planning and risk assessment

- Perceptions:
  - Entities appreciate public posting
  - Viewpoints on industry input vs. ERO Enterprise product
  - Significance to entities and impact to standards obligations
  - Audit approaches or auditors "shall follow"

- Disclaimer added:
  - Intended for ERO Enterprise staff
  - Developed exclusively by ERO Enterprise under obligations for independence and objectivity
  - Posted publicly solely for transparency

Questions and Answers

RELIABILITY | RESILIENCE | SECURITY

Compliance Monitoring and Enforcement Program Annual Report

James McGrane, Senior Counsel
Compliance Committee Meeting
February 9, 2022

**RELIABILITY | RESILIENCE | SECURITY**

- Roll out of Align and Secure Evidence Locker
- Continued focus on reliability and security despite coronavirus challenges
- Continued streamlining and enhancement efforts
  - Proposed changes to CMEP in September 2021 filing impacting:
    - Compliance monitoring
    - Resolution of minimal risk noncompliance
- Ongoing outreach to industry
  - Self-Logging
  - Compliance Oversight Plans
  - Facility Ratings
  - Proposed changes to Rules of Procedure

COVID-19 Logged Noncompliance Reported
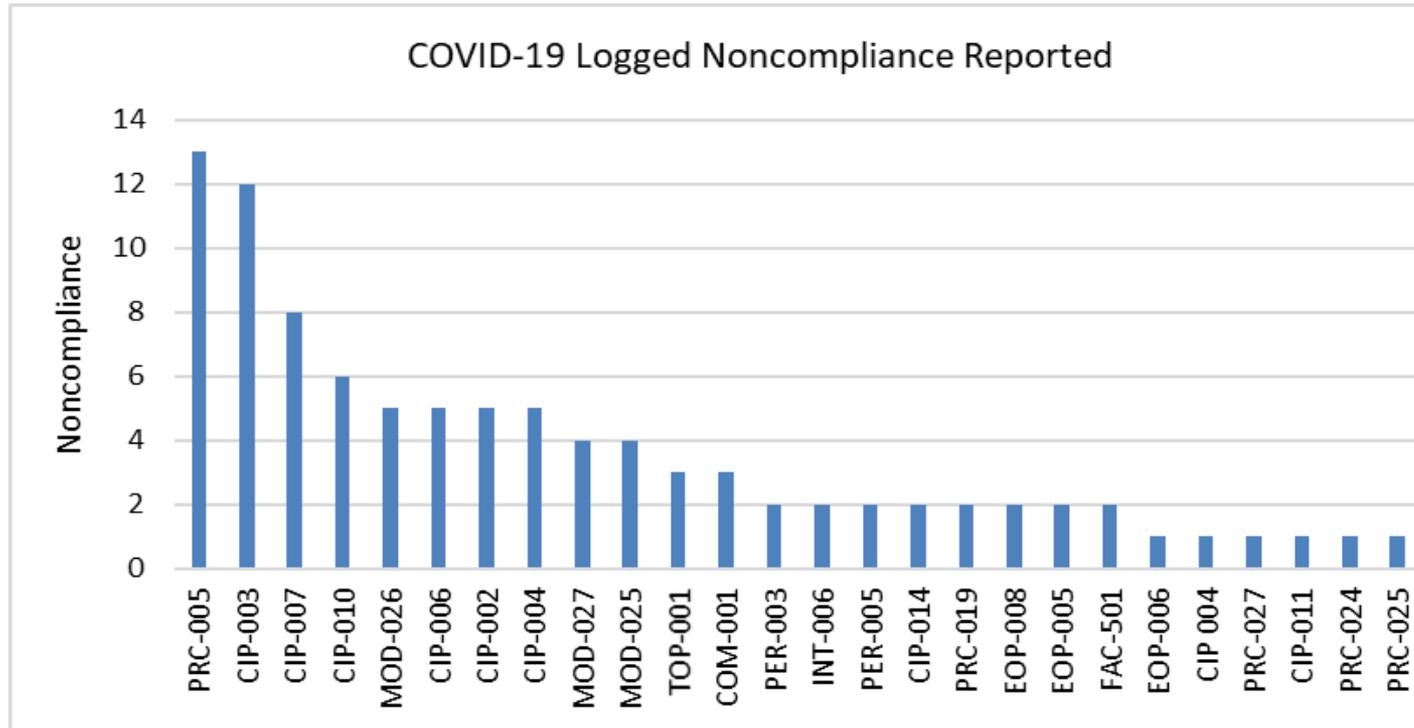
95 self-logged issues reported through December 31, 2021

- ## Supply Chain Risk Management
  - Stakeholder collaboration and outreach
    - ○ CCC Supply Chain Task Force
    - ○ FERC-NERC joint white paper on [SolarWinds and Related Supply Chain Compromise](#)

- ## Heightened focus on sharing best practices and guidance
  - Noncompliance reduction strategies
  - NIST-NERC collaboration and Standards mapping
  - Guidance to support Dept. of Energy 100 Day Cybersecurity Plan
  - Small Group Advisory Sessions (SGAS)
   - ○ CIP-012 Cyber Security – Communications between Control Centers

- Remote Connectivity
  - Maintenance and Vendor support
  - IT / OT communications and dependency

- Supply Chain
  - Foreign vendor component risk
  - Large impact

- Gaps in Program Execution
  - Incident Response identification and reporting

- Long Term Strategies
  - Continued focus on high risk areas (Connectivity, Supply Chain, Incident Response)
  - Outreach / Guidance around 2022 Focus Area findings and SGAS

RELIABILITY | RESILIENCE | SECURITY

Average Age of CIP and O&P Noncompliance in the ERO Enterprise Inventory by Quarter
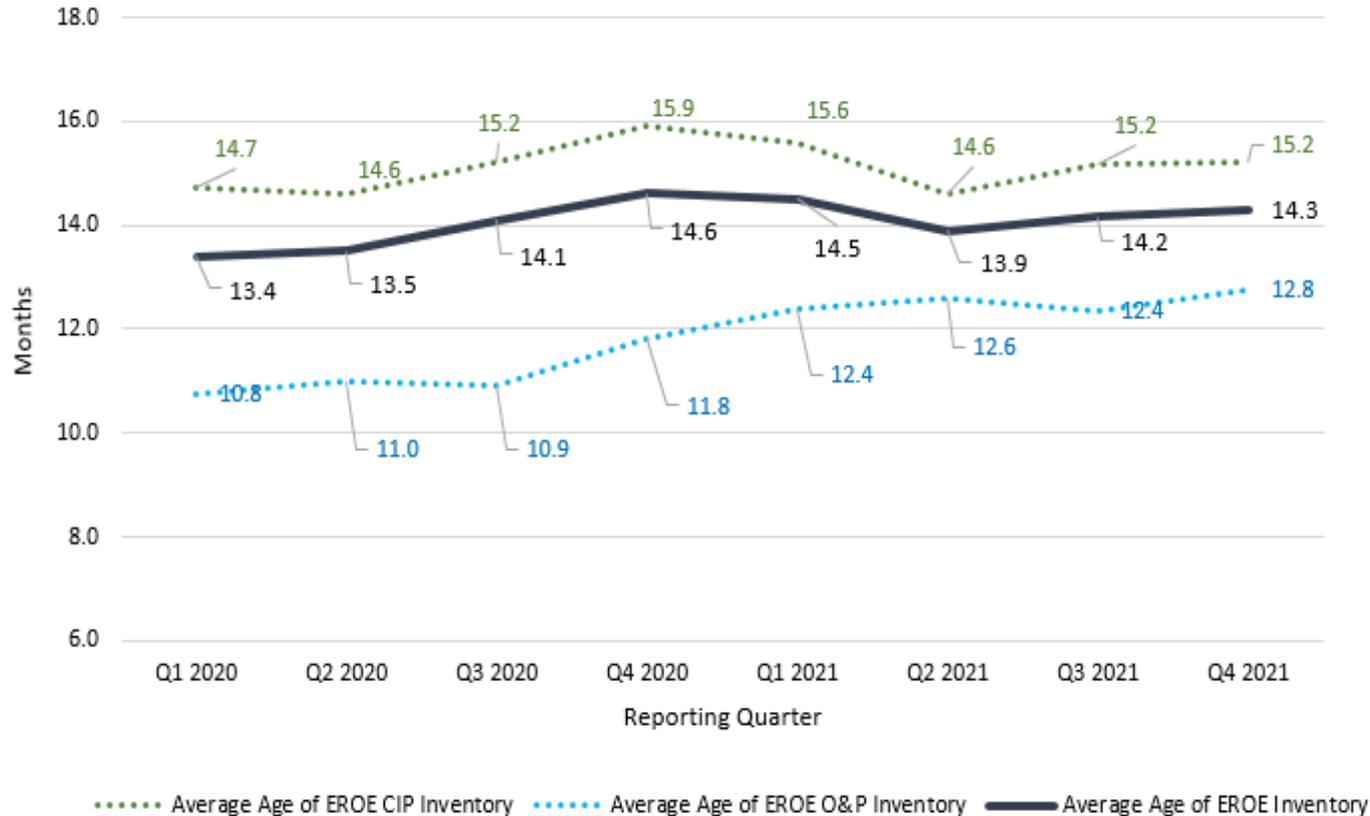
ERO Enterprise is taking steps to reduce average age of inventory

Percent of Noncompliance By Discovery Method for the Past 4 Quarters
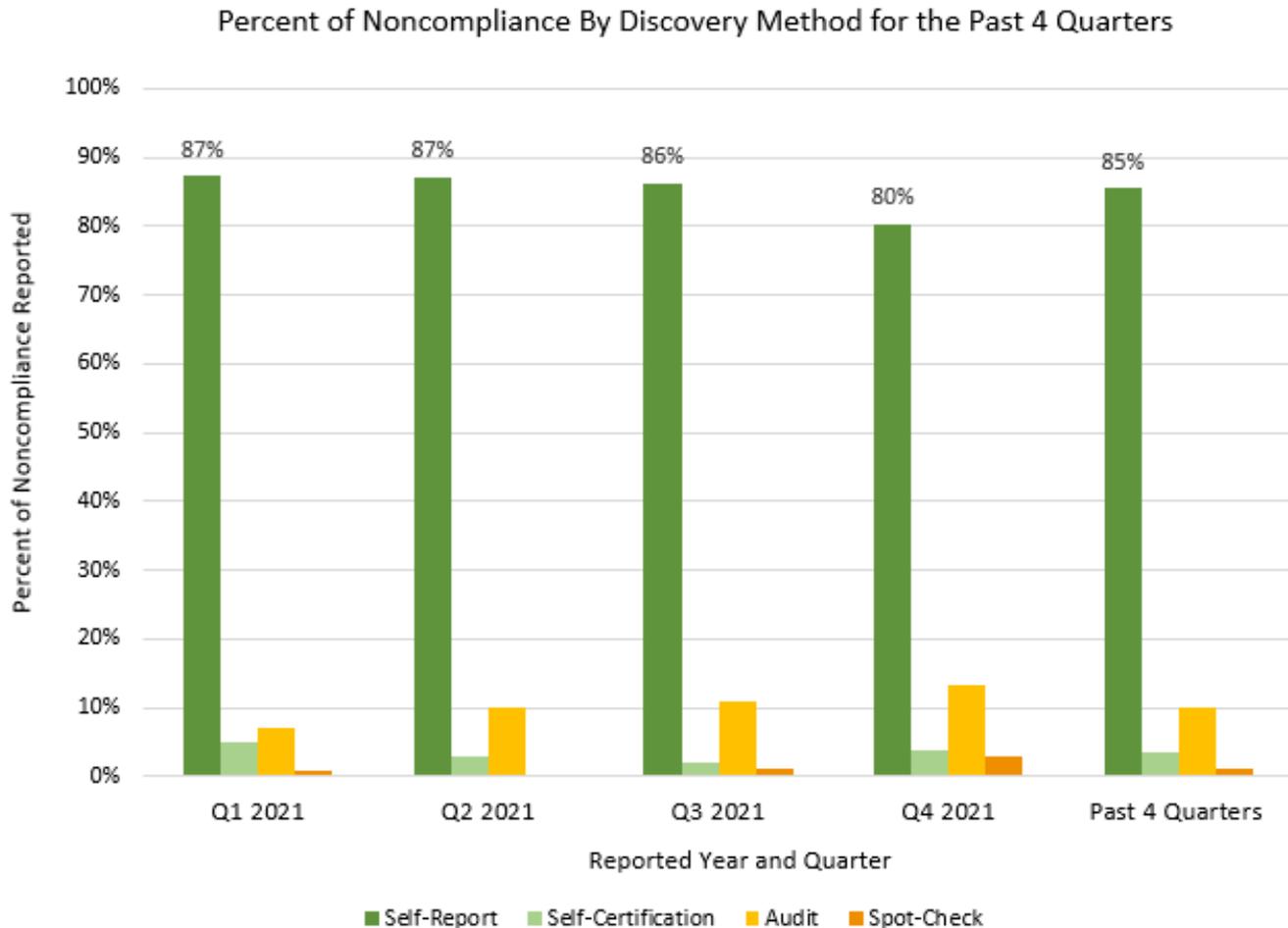
**Self-Reporting remains high, helping speed mitigation and reduce risk**

Time Frames for Completed Mitigations in the Past 5 years
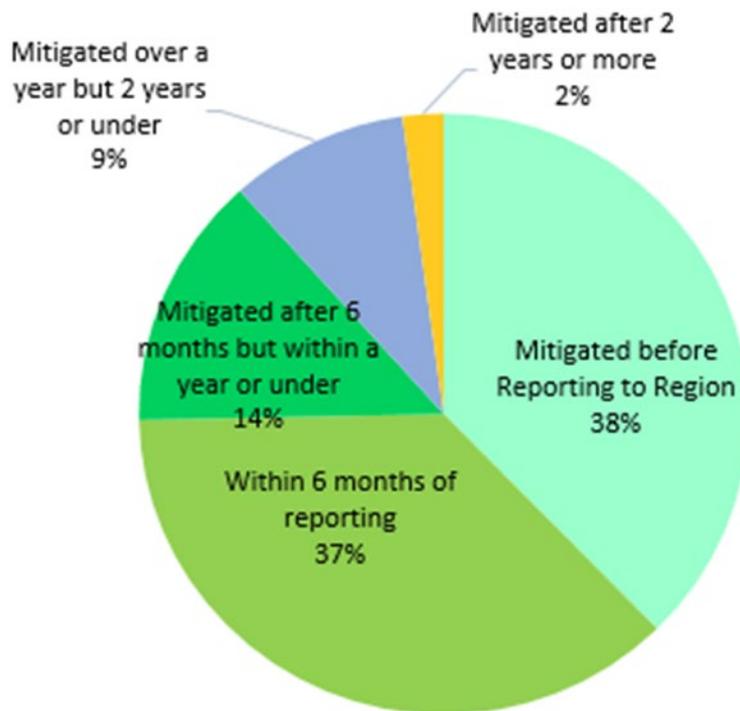
Majority of noncompliance is mitigated within one year of reporting

Disposition Breakdown for Filings from 2017 to 2021
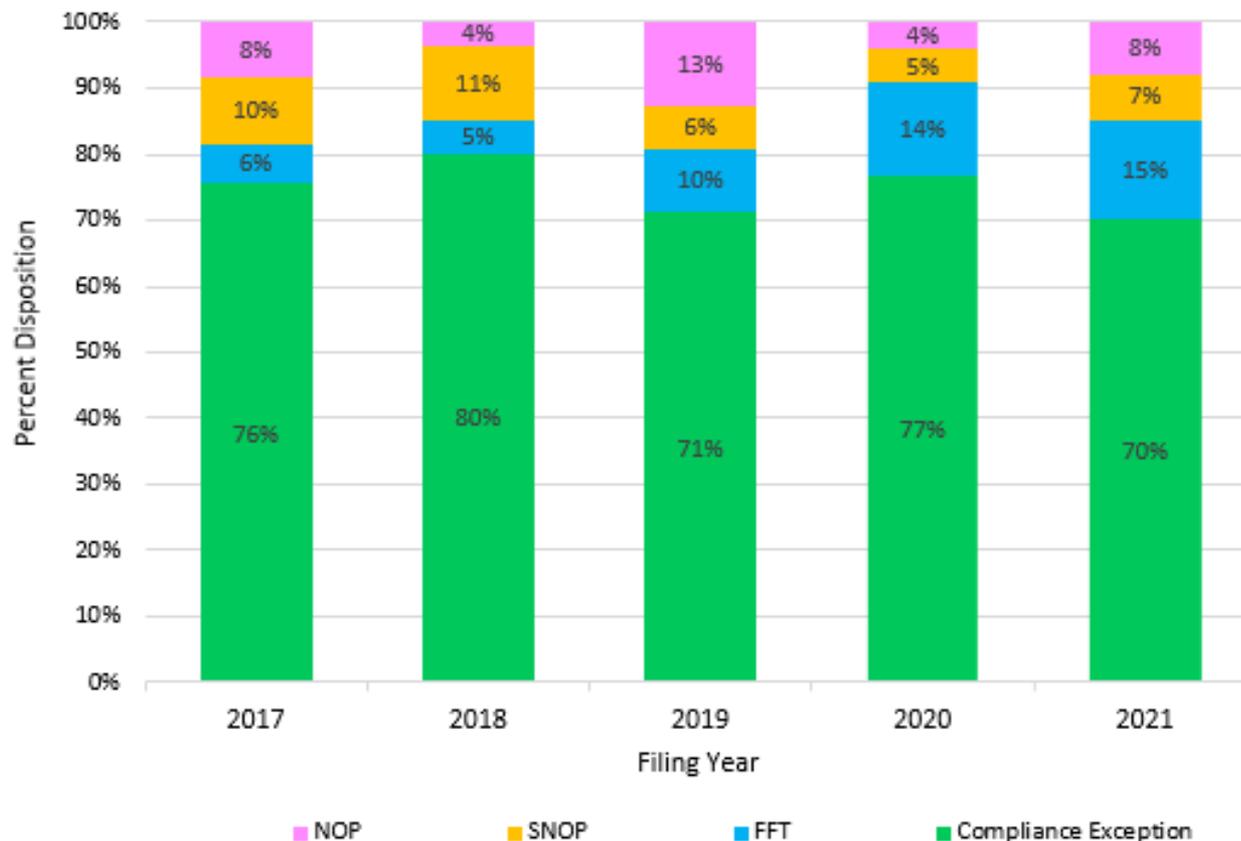
The majority of noncompliance continues to be processed as Compliance Exceptions

Percent Assessed Risk by Filing Year
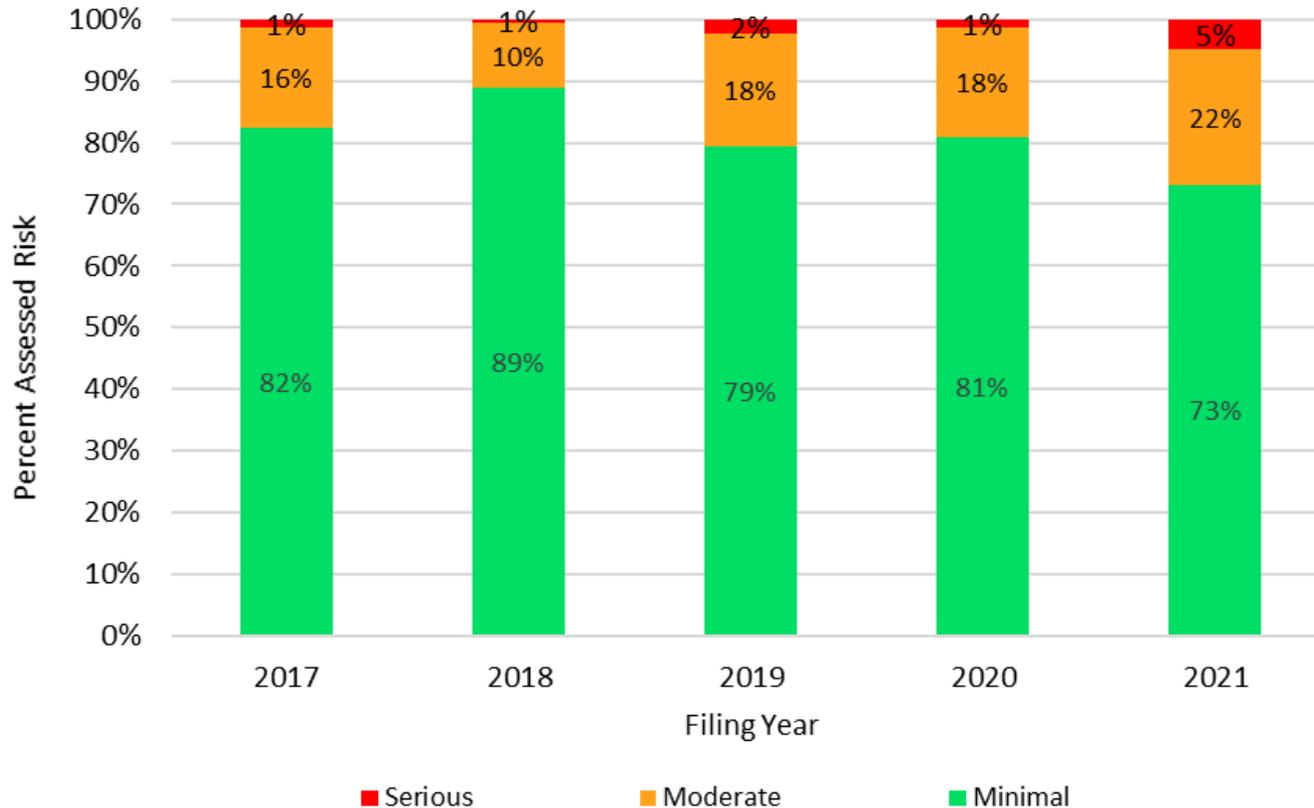
**Increase in serious risk noncompliance processed in 2021,
but majority had been mitigated prior to filing**

## Breakdown of Discovery Method for the Facility Rating Noncompliance Filings
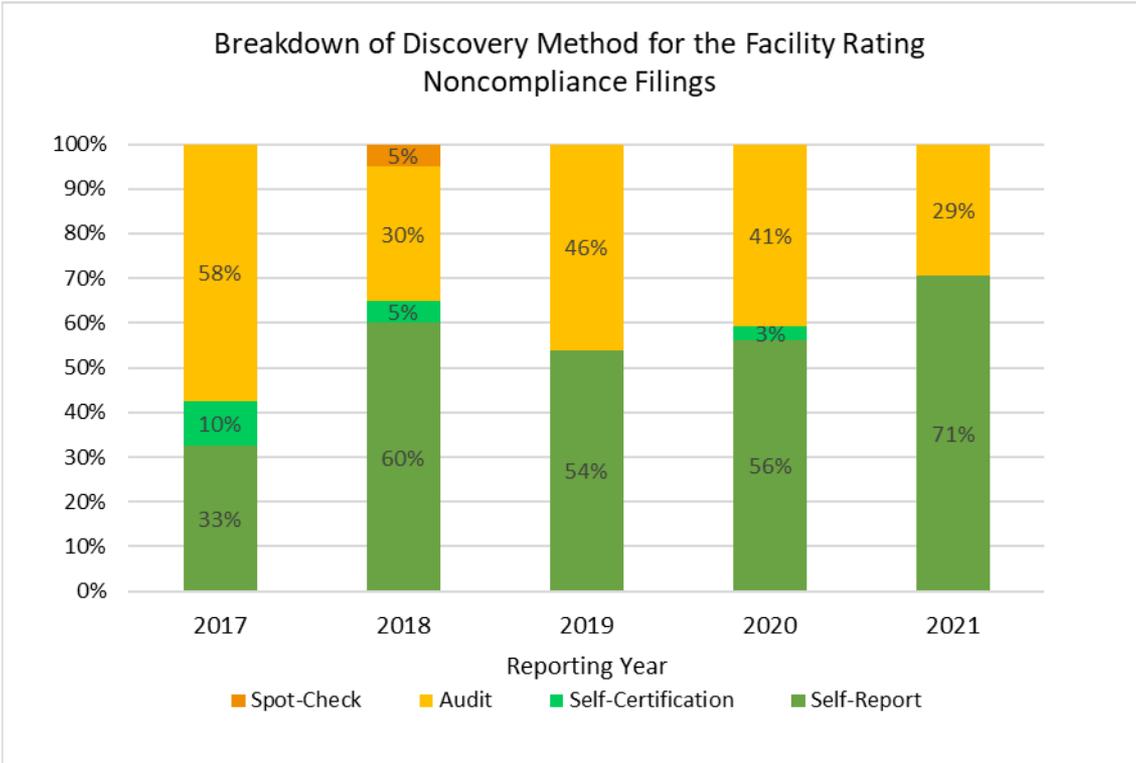
	2017	2018	2019	2020	2021	Total
Self-Report	13	12	14	18	24	81
Self-Certification	4	1	0	1	0	6
Audit	23	6	12	13	10	64
Spot-Check	0	1	0	0	0	1
Total	40	20	26	32	34	152

Increase in Facility Rating Self-Reports over last few years

Facility Rating Disposition Breakdown in the Past 5 Years
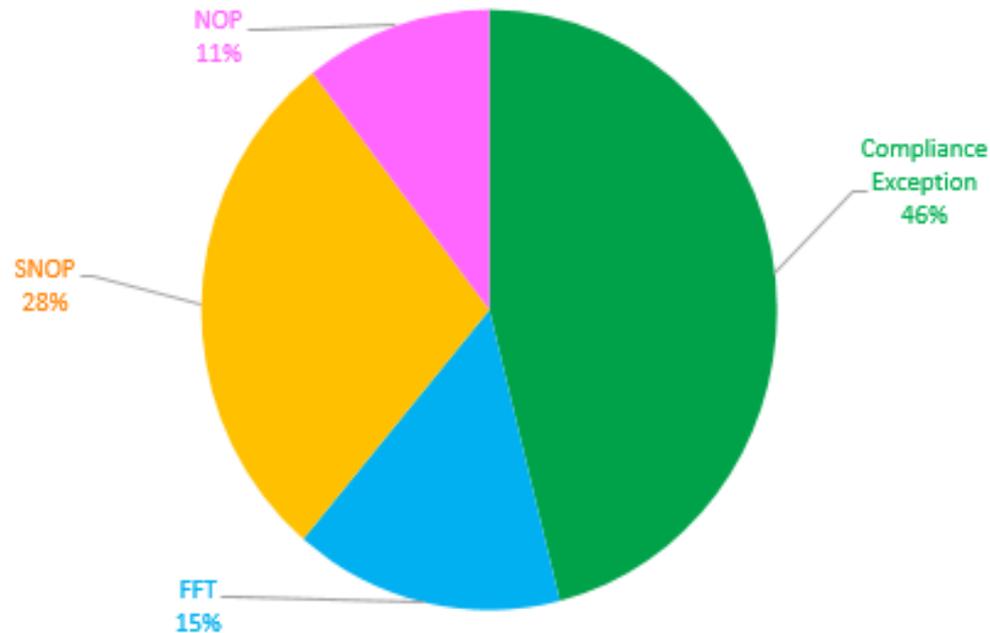
ERO Enterprise uses a risk-based approach in resolving Facility Rating noncompliance

- Streamlining efforts
  - Efficient risk assessment and resolution for all noncompliance
  - Sharing approaches across Regions to identify processing efficiencies

- Ongoing engagement with registered entities
  - Understanding extent of violations and assisting the design of robust controls to prevent recurrence

- Sharing lessons learned and mitigation best practices
  - Effective solutions to the most common causes of violations
  - Outreach on new Reliability Standards and preventive controls

RELIABILITY | RESILIENCE | SECURITY

Questions and Answers

RELIABILITY | RESILIENCE | SECURITY