



RELIABILITY **FIRST**

**Theme: Protecting/Securing the Grid of the Future**

# Agenda

## Board of Directors

August 22, 2024 • 8:00 am – 12:30 pm (ET)

**Gervasi Vineyard**

**1700 55<sup>th</sup> Street NE • Canton, OH 44721**

**Room: Villa Grande Ballaria Sophia**

**Attire: Casual**

### Closed Agenda

#### Board of Directors – Executive Session

- 1. **The Interregional Transfer Capability Study Update** 8:00 am  
 Presenter: Jim Uhrin, Director Engineering & Reliability Services
- 2. **Confidential Security Update** 8:10 am  
 Presenter: Marcus Noel, VP and CSO
- 3. **Gas Industry Training Part II** 8:20 am  
 Presenter: Michael Oberleitner, Fuel Commodity Specialist, Dominion Energy  
 Reference: Presentation
- 4. **Confidential Executive Session** 9:15 am  
 Presenter: Antonio Smyth, Chair

### Open Agenda

- 1. **Call to Order and Appoint Secretary to Record Minutes** 9:45 am  
 Presenter: Antonio Smyth, Chair
  - 2. **Antitrust Statement** 9:48 am  
 Presenter: Niki Schaefer, Vice President and General Counsel  
 Reference: Antitrust Compliance Guidelines
  - 3. **Consent Items** 9:50 am  
 Presenter: Antonio Smyth, Chair  
 Reference:
    - a) [Draft Minutes from May 2, 2024](#)
    - b) [Draft Minutes from June 27, 2024](#)
    - c) [Resolution to Hold Annual Meeting of Members \(No.2024-03\)](#)
    - d) ERO Enterprise Long-Term Strategy (for endorsement)
    - e) [2025 Proposed Board Meeting Dates](#)
- Action: **Approve Consent Items**

4. **Keynote Speaker** 9:55 am  
 Presenter: Kurtis Minder, CEO and Co-Founder GroupSense  
 Reference: [Bio](#)
5. **Guest Speaker** 10:20 am  
 Presenter: Colleen Sidford, NERC Board of Trustees  
 Reference: [Bio](#)
6. **President's Report** 10:40 am  
 Presenter: Tim Gallagher, President and CEO  
 Reference: [Impact Report](#)
- Break** 11:00 am
7. **CIP Themes Report** 11:10 am  
 Presenter: Tom Scanlon, Managing Enforcement Counsel  
 Description: Mr. Scanlon will provide an overview of the 2024 ERO CIP Themes Report, which discusses key risk themes identified through monitoring and enforcement activities.  
 Reference: a) [Presentation](#)  
 b) [2024 ERO CIP Themes Report](#)  
 Action: Information and Discussion
- 11:20 am
8. **Standing Updates** (Information provided for transparency into key aspects of RF operations) 11:30 am  
**[Financial](#)**  
 Beth Dowdell, Senior Director, Corporate Services will provide an update on the Q2 financials including variances and year-end projections. She will also provide a procedural update on the business plan and budget.
- [Security](#)**  
 Marcus Noel, CSO, will provide an organizational security update.
9. **Committee Reports** 11:50 am  
*Talent and Compensation Committee • Lesley Evancho*  
*Risk and Compliance Committee • Joanna Burkey*  
*Finance and Audit Committee • Patrick Cass*  
*Nominating & Governance Committee • Rachel Snead*
10. **Stakeholder Comments** 12:20 pm
11. **2024 Future Meetings:** 12:25 pm  
 • December 4-5 • Washington, DC
12. **Adjourn and Lunch to follow** 12:30 pm

**Roster • Board of Directors**

Antonio Smyth, **Chair** • AEP (S • 2026)  
Nelson Peeler, **Vice Chair** • Duke Energy (T • 2024)  
Patrick Cass • **Lead Independent** (2026)  
Steve Ambrose • DTE Energy (M-LSE • 2025)  
Joanna Burkey • Independent (2025)  
Melika Carroll • Independent (2027)  
Lesley Evancho • Independent (2025)  
Tim Gallagher • ReliabilityFirst  
Scott Hipkins • FirstEnergy Services Company (T • 2024)  
Ken Seiler • PJM (RTO • 2024)  
Rachel Snead • Dominion Resources Services, Inc. (S • 2024)  
Jennifer Sterling • Exelon Corporation (L-LSE • 2025)  
Robert Taylor • Invenergy (AL • 2026)  
Joe Trentacosta • Southern Maryland Electric Cooperative, Inc. (AL • 2025)  
Simon Whitelocke • ITC Holdings Corporation (AL • 2024)

# **a) 2024-05-02 DRAFT Board of Directors Minutes**



RELIABILITY FIRST

PUBLIC

## Draft Minutes Board of Directors

May 2, 2024

ReliabilityFirst Corporation  
3 Summit Park Drive, Suite 600 • Cleveland, OH 44131

---

### Closed Session

**Executive Session** – The ReliabilityFirst (RF) Board of Directors met in executive session at 8:00 am (ET) and discussed confidential matters concerning the corporation. Presentations included an update on the status of the interregional transfer capability studies being performed by the ERO pursuant to the Fiscal Responsibility Act of 2023 and a confidential security update.

---

### Open Session

**Call to Order** – Chair Smyth called to order a duly noticed open meeting of the Board of Directors (Board) at 9:04 am, consisting of the following members of the Board: Chair Antonio Smyth; Vice Chair Nelson Peeler; Steve Ambrose; Joanna Burkey; Patrick Cass; Lesley Evancho; Tim Gallagher; Craig Grooms; Ken Seiler; Rachel Snead; Jennifer Sterling; Joe Trentacosta; and Simon Whitelocke.

A list of others present during the Board meeting is set forth in Attachment A.

**Appoint Secretary to Record Minutes** – Chair Smyth designated Niki Schaefer, RF's Vice President and General Counsel, as the secretary to record the meeting minutes.

**Antitrust Statement** – Ms. Schaefer advised all present that this meeting is subject to, and all attendees must adhere to, RF's Antitrust Compliance Guidelines.

**Consent Items** – Chair Smyth introduced the following consent agenda items for approval:  
Agenda Item 3(a): Draft Minutes from December 7, 2023 Annual Meeting of Members  
Agenda Item 3(b): Draft Minutes from December 7, 2023 Board of Directors Meeting  
Agenda Item 3(c): Draft Minutes from March 26, 2024 Board of Directors Meeting  
Agenda Item 3(d): Resolution to Hold Industry Elections (No. 2024-01)

Upon a motion duly made and seconded, the Board approved the consent agenda items.

**Keynote Speaker** – Chair Smyth introduced the keynote speaker, Dr. Elizabeth Cook, VP Technical Strategy of AIC. Dr. Cook discussed her career in the electric industry, and the risks and challenges the electric grid is presently facing, particularly related to the proliferation of distributed energy resources (DER) and artificial intelligence (AI). She noted that the items at the edge of the BES (like DER) can potentially affect the BES. Dr. Cook then noted that the world is in the midst of a transformation in energy, supply chain, and how we receive and use information. For example, solar, batteries, electric vehicles, and demand response are rapidly becoming available at scale.

Dr. Cook noted the large demand for electricity coming from AI data centers (and the risks associated with that extra demand) but also discussed the potential benefits of AI for the grid. For example, because AI can predict future patterns and fill in information, it could provide additional insight on how to increase grid capacity, efficiency, and stability. She also noted that load forecasting is continuously evolving with the use of AI. She emphasized the importance and power of data, and how each utility is in a varying state of maturity in how they use their data.

Chair Smyth asked about how to encourage customers to participate in efficiency programs, and Dr. Cook stated that this is a change management effort and can be difficult without the proper regulatory incentives in place for utilities and individuals. In response to a question about DER cybersecurity, Dr. Cook stressed the importance of educating vendors and developers on cybersecurity and the CIP Standards.

**President's Report** – Tim Gallagher, RF's President and CEO, welcomed Craig Grooms to the Board and thanked Howard Gugel and all the guest speakers for coming to the meeting. He discussed the ERO Roadmap for NERC and the Regions, which is being converted into a strategic plan that will be endorsed by the Regions and issued in July. He then discussed the recent retreat for NERC and Regional CEOs, and an upcoming strategic session with the NERC Board and Regional Board officers. There was also a recent retreat for RF management, which focused on staff development and performance management. Mr. Gallagher reported that the latest employee engagement survey had an 85% employee engagement level and 98% response rate, both of which are very high.

Mr. Gallagher then discussed the success of RF's state outreach efforts, noting that RF is being asked by state senators (both within and outside of our Region) to meet and provide expertise. He also noted that he spoke at a recent AEP compliance seminar that included discussion on the reliability impact of large load demands from data centers. Mr. Gallagher stated that he would like to bring in an expert to discuss this topic with the Board, and Chair Smyth agreed, noting that AEP will be testifying on this topic in Congress. There was also a recent joint meeting with the ERO and the North American Transmission Forum, which featured a presentation from a chief meteorologist from CISA on how weather influences critical infrastructure – he would like to have a similar presentation for the Board on this topic as well.

Mr. Gallagher thanked RF's Managing Enforcement Counsel Tom Scanlon for leading efforts to update RF's CIP themes report in partnership with the other Regions. He noted that Mr. Scanlon can provide the Board with a briefing on the report. He also thanked Beth Dowdell, Senior Director Corporate Services, and Christi Klein, Manager Finance & Accounting, for their efforts on RF's 2025 Business Plan & Budget, and thanked Ms. Evancho for her guidance on resource planning. RF also had a clean financial audit this year, with efforts led by Ms. Dowdell, Ms. Klein, and Mr. Cass. He concluded his remarks by thanking the team (Ms. Burkey, Mr. Cass, Ms. Sterling, Mr. Whitelocke, Ms. Schaefer, Ms. Dowdell, and Ms. Tortora) that is recruiting for the open independent director position and has identified many excellent candidates so far.

**2023 ERO Reliability Risk Priorities Report** – Howard Gugel, NERC's Vice President of Compliance Assurance and Registration, discussed the 2023 ERO Reliability Risks Priorities Report (Report) and the ERO's risk framework. This framework includes risk identification, validation, prioritization, mitigation, and monitoring, and involves different groups such as the Compliance and Certification Committee, Standards Committee, and the Reliability and Security Technical Committee. He then discussed the Reliability Issues Steering Committee (RISC), its objectives, and biennial activities.

Mr. Gugel gave an overview of five high-level risk profiles from the Report: security risks, grid transformation, resilience and extreme events, critical infrastructure interdependencies, and energy policy. He noted that energy policy is a new risk profile, and an example of this would be a policy which results in reliability issues when implemented. Mr. Gugel then discussed how the RISC conducts risk ranking with experts and reported that the changing resource mix was the top ranked risk for 2023. The Board discussed how the Report relates to the RF Regional Risk Assessment report. RF Senior Vice President Jeff Craig noted that RF considers the Report when working on the Regional Risk Assessment, but that RF looks at data specifically in the RF region.

**Inverter-Based Resources** – Mr. Gugel then discussed risks associated with inverter-based resources (IBRs). He discussed the need for wide-area energy assessments, illustrated by a June 2023 "wind drought" in ERCOT, SPP, and MISO during which 60 GW of installed wind capacity only generated 300 MW. He also discussed how 100 MW of baseload generation compares to hybrid (*i.e.*, solar plus batteries), and that more hybrid MW is required to replace baseload MW. Mr. Gugel described how the future will be "decarbonized, digitized, and distributed," and how it is important to manage the pace of transformation to ensure reliability. He stressed the importance of developing sufficient transmission to integrate renewables and ensuring the availability of essential reliability services and a robust energy supply chain.

He then gave an overview of NERC's IBR strategy and activities, including the FERC order requiring NERC to register bulk power system-connected IBRs, and NERC's work plan in response to that order. Mr. Gugel also discussed the IBR communication plan, which includes an IBR quick reference guide, quarterly updates, and webinars. Mr. Whitelocke asked about the batteries supporting IBRs, and Mr. Gugel responded that there is not yet lot of data on this because of the small number of battery installations. There was discussion on how winter weather can decrease battery quality and output, and how the

industry should study whether additional batteries should be installed for the winter season to mitigate this risk.

**Resource Adequacy** - Davey Lopez, Lead Resource Adequacy Planning at MISO and Asanga Perera, Sr. Manager of Planning at PJM, discussed resource adequacy studies and projections in the MISO and PJM footprints. Mr. Lopez discussed how MISO is entering a different risk paradigm with increasing extreme weather events and the transition to renewables. He reported that MISO projects a capacity shortfall beginning in 2025-2026, that capacity additions are needed, and retirements may need to be delayed. He stated that MISO is projected to meet most 2024-2025 resource adequacy requirements, but pressure persists with overall reduced capacity surplus and a shortfall in MISO's Zone 5 (around Missouri). Mr. Lopez then discussed MISO's resource adequacy initiatives such as adjusting seasonal planning reserve margin requirements and maturing information exchange, modeling, and gap analysis to better inform resource investment and retirement. He described how last year MISO moved from an annual to a seasonal resource adequacy construct, with risk-based accreditation for all resources (measuring the resource's availability when the reliability risk is the greatest). Mr. Seiler asked if there are resource adequacy backstops, and Mr. Lopez noted that the reliability-based demand curve and the reforms to the capacity market help to act as a backstop.

Mr. Perera then provided a resource adequacy update from PJM. He shared PJM's load growth forecasts and reported that load growth is projected to increase over time. Mr. Perera then noted that resource retirements and load growth could outpace new entry, causing resource adequacy risks to emerge by 2028-2030. He discussed that PJM's 2030 load forecast has gone up by 10 GW since last year due to the growth in demand from data centers and electrification. Additionally, PJM's generation retirement projections are the same as last year, but PJM is now projecting an additional 2 GW in new capacity compared to last year's forecast (mostly coming from gas). Mr. Perera stated that the PJM markets will respond to the decreasing reserves with higher prices, which could result in additional supply and fewer retirements. He also noted that reforms to the PJM energy and capacity market reforms are underway. Mr. Perera then discussed how in the policy space, PJM is encouraging policymakers to avoid retirement policies until adequate supply is available and create safety valves to keep plants open if needed. In the planning space, PJM is executing interconnection planning reforms, which has resulted in over 100 GW of interconnection service agreements. Ms. Sterling noted that most of the resource adequacy risk comes from the risk of generation retiring due to clean energy and affordability policies.

**Financial Update** – Ms. Dowdell provided a financial update. She discussed the recent financial audit of RF, which was a clean audit with no deficiencies or issues. She then discussed the first quarter financials, which are 3.22% under budget. Ms. Dowdell also provided key first quarter budget variances, with funding \$67K above expected due to strong returns in the market. She noted that personnel expenses are down by \$136K due to reduced healthcare costs, and that meetings and travel expenses are down \$43K based on the timing of events through the year. She shared that operating expenses are down \$316K due to the timing of consultant and contractor use, and due to having fewer independent directors in place during the first quarter. Finally, Ms. Dowdell reported that rent and utilities were anticipated to be higher than they were in the first quarter. She



Dowdell then discussed the year-end projections, including predictions that funding and personnel may be over budget; meeting expenses may be on target, and that operating expenses may be under budget due to the recent lower cost of rent and utilities.

Ms. Dowdell discussed the draft 2025 Business Plan and Budget (BP&B), which was included in the agenda package. She first provided the low and high-range budget projections from last year (4.3% and 6.5%, respectively), and reported that RF landed at a 6.5% budget increase for the 2025 BP&B, driven by the addition of three new FTEs. Ms. Dowdell reported that assessments are increasing by 6%, and shared that personnel expenses make up 86% of the 2025 BP&B. She then discussed budget variations from 2024 to 2025. In response to a question about a budgeted increase in office costs, Ms. Dowdell explained that this is due to an increase in IT/technology expenses. She compared budget, FTE, and assessment increases across the Regions, reporting that RF falls on the low end in all these categories across the Regions.

Ms. Dowdell noted the internal reductions made by RF to optimize the 2025 BP&B. This included keeping travel expenses flat from 2024 (saving about \$78K), staggering the start dates for FTEs (saving about \$50K), reducing contractor costs (saving about \$300K), and keeping meeting expenses flat (saving about \$130K). She then provided the 2026 and 2027 budget projections, with a 5.6%-8.5% increase for 2026, and a 3.3%-7.7% increase for 2027. Ms. Dowdell completed her presentation by discussing RF's history of budget vs. assessment increases, and the ongoing assessment stabilization effort to minimize large fluctuations in assessments to stakeholders.

Chair Smyth requested Board approval of the draft 2025 BP&B, for a 30-day posting for stakeholder comment and submittal to NERC. Mr. Cass noted that the Finance and Audit Committee unanimously endorsed the approval of the draft 2025 BP&B. Upon a motion duly made and seconded, the Board approved the posting of the draft 2025 BP&B for stakeholder comment and submittal to NERC. Ms. Dowdell noted that on or before June 30th, the Board will review and approve the final 2025 BP&B.

**Security Update** – Marcus Noel, RF's Vice President and Chief Security Officer, provided a security update. He discussed the results of a peer maturity comparison, during which RF self-assessed its maturity in 50-60 areas to obtain a NIST CSF capability level. He shared a graph showing RF's maturity compared to the Gartner peer group, and RF consistently outperformed the peer group across the different security capabilities. Mr. Noel then discussed how RF wants to keep maturing the Identify, Detect, and Recover security capabilities in 2024 and beyond. He shared recent activities in these areas, such as testing recovery plans and expanding monitoring and alerting capabilities. Mr. Noel noted that the security team and executive team will be further discussing what acceptable risk looks like and investing time on the residual risks.

**Outreach and Regulatory Update** – Diane Holder, Vice President of Entity Engagement and Corporate Services, provided an update on RF's state outreach efforts. She shared that the state outreach program is thriving, and a focus on customized messages has resulted in deeper discussions with states. She reported that RF has recently provided testimony at hearings in several states, including Pennsylvania, Ohio, West Virginia,

Maryland, and Illinois. Ms. Holder noted that RF's objectivity and role as a technical resource for the states is a fundamental principle and a key strength that sets RF apart to the states. RF also has one on one meetings with state commissions, and NARUC is a key venue for meetings as it allows RF to talk to multiple states at once. She also reported that RF has conducted state-focused RF Tech Talks, issues a State Energy Insights monthly newsletter, and is planning a legislative panel for the RF Fall Summit in September. Ms. Holder discussed the increase in state "in-reach," meaning when RF receives requests from state legislators and officials to come to meetings, testify, present, or comment on upcoming initiatives. She shared that blackstart resources, load growth, and resource adequacy are popular topics that the states request RF's expertise on. Ms. Holder then provided some policy updates, giving summaries of the Big Wires Act, the Good Neighbor Plan, and the EPA standards for fossil fuel plants. Mr. Grooms asked if RF or NERC provided comments on the EPA's fossil fuel plant standards, and Ms. Holder replied that RF did not provide comments and she does not think that NERC did either. Finally, Ms. Holder discussed next steps for the state outreach program, which includes the creation of state outreach scorecards and discussion on how to define and measure success.

## **Committee Reports:**

### **a) Talent and Compensation Committee**

Talent and Compensation Committee Chair Lesley Evancho reported that the Committee received an update from HR Manager Hue Deluca on key talent metrics, and that the staff diversity demographics are either flat or positively trending. The Committee discussed how RF has a low turnover rate and is doing a good job of getting and keeping talent. Ms. Deluca also shared that RF has an 85% staff engagement score, which is high and resulted in RF being named as a top employer in Northeast Ohio. RF's HR department is currently looking at comments from the engagement survey, and any potential improvements to make resulting from it. The Committee received information on RF's new 8-week summer internship program, and discussed RF's new diversity strategy to foster a company culture that pursues and attracts diverse and top-notch talent, recognizes individuals for their contributions, and allows employees to feel comfortable being themselves at work. Ms. Dowdell then discussed the tier 1 and 2 corporate goals for 2024 and reported that the corporate goals are currently on track for timely completion. Finally, Ms. Schaefer discussed a recent strategic session of the RF executive team that focused on what types of work across the organization to stop/start/continue/improve. As a result of that session, teams will be working on innovating or restructuring certain business processes and will report the results to Mr. Gallagher and to the Compensation Committee.

### **b) Risk and Compliance Committee**

Risk and Compliance Committee Chair Joanna Burkey reported that the Committee received a presentation from RF's Manager of Engineering Johnny Gest on RF's Regional Risk Assessment report (RRA) and process. During that presentation, Mr. Gest discussed the directionality of risks, including that misoperations are down and risks related to the changing resource mix and environmental regulations are ranked the highest. The Committee then received an update from Mr. Scanlon on enforcement metrics and trends,

and emerging operational risks like vegetation management. Manager of External Affairs Michelle Cross then led a discussion on the planned retirement of the Brandon Shores and Wagner Power Plants in Maryland, and how generator plan retirements are contributing to resource adequacy risks. The Committee also received an overview of RF's delegated authority from NERC, and how NERC oversees those delegated activities. The Committee enjoyed this presentation and requested that it be included in director onboarding going forward. Finally, in closed session the Committee discussed confidential compliance and enforcement matters with RF staff.

### **c) Finance and Audit Committee**

Finance and Audit Committee Chair Pat Cass reported that the Committee met with Mandy Pittman from RF's external accounting firm RSM US LLP, who presented the results of the 2023 financial audit. The Committee then approved the audited financial statements, and met with Ms. Klein, the new Manager of Finance and Accounting. The Committee reviewed RF's investment portfolio, which is invested in short term assets (mostly treasury and bonds). In closed session, the Committee discussed the first draft of the 2025 Business Plan and Budget and endorsed it for Board approval. Additionally, the Committee had an executive session with Ms. Pittman about the financial audit, and she was very complimentary of RF.

### **d) Nominating & Governance Committee**

Nominating and Governance Committee Chair Rachel Snead reported that the Committee reviewed the timetable of RF key events and the results of the Board biennial self-evaluation. The Committee also endorsed the resolution to hold elections for the At-Large and Independent Directors and endorsed Robert Taylor, Vice President of Transmission New Markets at Invenergy as the At Large Director candidate. She provided background information on Mr. Taylor, who has also led transmission strategy at Exelon. Upon a motion duly made and seconded, the Board approved the nomination of Mr. Taylor as the At-Large Director candidate.

**Next Meeting** – Chair Smyth noted that the next meeting of the Board of Directors will occur on August 22, 2024.

**Adjourn** – Upon a motion duly made and seconded, Chair Smyth adjourned the meeting at 12:33 pm (ET).

As approved on this 2nd day of May 2024, by the  
Board of Directors,

Niki Schaefer  
*Vice President, General Counsel & Corporate  
Secretary*

**ATTACHMENT A**

---

**Others Present During the Board of Directors Meeting**

Elizabeth Cook  
Jeff Craigo • ReliabilityFirst  
Michael DeVisco • PJM  
Beth Dowdell • ReliabilityFirst  
Chelsey Eppich • ReliabilityFirst  
Tom Foster • PJM  
Megan Gambrel • ReliabilityFirst  
Howard Gugel • NERC  
Vinit Gupta • ITC  
Doug Hohlbaugh • First Energy  
Diane Holder • ReliabilityFirst  
Davey Lopez • MISO  
Price Marr • PJM  
Kamila Molda • PJM  
Marcus Noel • ReliabilityFirst  
Asanga Perera • PJM  
Tony Purgar • ReliabilityFirst  
Niki Schaefer • ReliabilityFirst  
Kristen Senk • ReliabilityFirst  
Matt Thomas • ReliabilityFirst  
Jody Tortora • ReliabilityFirst  
Jim Uhrin • ReliabilityFirst

## **b) 2024-06-27 Draft Board of Directors Minutes**

**RELIABILITY FIRST**

## **DRAFT - Minutes**

### **Board of Directors Teleconference**

June 27, 2024 • 3:00 pm – 4:00 pm (ET) • Virtual

**ReliabilityFirst Corporation**

**3 Summit Park Drive • Cleveland, OH 44131**

---

#### **Closed Session**

**Call to Order** – Vice Chair Nelson Peeler called to order a duly noticed closed meeting of the Board of Directors (Board) on June 27, 2024, at 3:02 (ET). A quorum was present, consisting of the following members of the Board: Steve Ambrose; Joanna Burkey; Patrick Cass; Lesley Evancho; Tim Gallagher; Craig Grooms; Scott Hipkins; Rachel Snead; Jennifer Sterling; Joe Trentacosta; and Simon Whitelocke.

A list of others present during the Board meeting is set forth in Attachment A.

**Appoint Secretary to Record Minutes** – Vice Chair Peeler designated Niki Schaefer, ReliabilityFirst's (RF) Vice President and General Counsel, as the secretary to record the meeting minutes.

**Antitrust Statement** – Ms. Schaefer advised all present that this meeting is subject to, and all attendees must adhere to, RF's Antitrust Compliance Guidelines.

**2025 Business Plan and Budget** – Beth Dowdell, RF's Senior Director Corporate Services, presented the final 2025 Business Plan and Budget (2025 BP&B) to the Board. Ms. Dowdell began by restating the budget numbers, which remained unchanged from the initial draft of the 2025 BP&B. Minor revisions were made to the language of the document, including clarifying RF's range of budget projections. Ms. Dowdell shared that the budget was posted for comment, and once approved it would go to NERC's Board in August and then to FERC most likely in October 2024. Ms. Dowdell compared RF's budget with other regions, noting that RF's increase is the second lowest across the regions. There was a discussion on the release of reserves impacting other region budgets. Upon a motion duly made and seconded, the Board adopted Resolution No. 2024-02 to approve the final 2025 BP&B.

**Independent Director Candidate** – Joanna Burkey presented the Independent Director candidate on behalf of the search committee. She shared the process for finding candidates, and the profile the search committee selected: a policy expert from a critical infrastructure industry with significant time to invest in the RF Board. Then she shared the process of narrowing down and selecting a final candidate through a process of multiple rounds of virtual and in-person interviews. Ms. Burkey presented Melika Carroll, the Nominating and Governance Committee endorsed candidate, and shared her background and expertise. Ms. Burkey shared that Ms. Carroll's current role at Cohere, an Artificial Intelligence ("AI") platform company, gives her an

**Board of Directors Minutes  
June 27, 2024**

understanding of both AI technology and also the energy needs of players in the AI space. Additional comments were made, noting Ms. Carroll's impressive preparations and thoughtful questions throughout the interview process. Ms. Burkey then covered next steps, including the ballot for the member election on July 30<sup>th</sup> to allow for a condensed onboarding for Ms. Carroll before her attendance at the August RF meeting. Lead Independent Pat Cass will also do an independent onboarding, and then a larger Board training will occur in early 2025. Mr. Cass then asked for a motion to approve Ms. Carroll as an Independent Director, which was made, seconded and unanimously approved.

**Next Meeting** – Vice Chair Peeler noted that the next Board meeting will be held on August 22, 2024, in Cleveland, OH.

**Adjourn** – Upon a motion duly made and seconded, Vice Chair Peeler adjourned the meeting at 3:45 (ET).

As approved on this 22<sup>nd</sup> day of August, 2024 by the  
Board of Directors,

Niki Schaefer  
*Vice President General Counsel & Corporate  
Secretary*

## Attachment A

---

### Others Present During the Meeting

Jeff Craig • ReliabilityFirst  
Beth Dowdell • ReliabilityFirst  
Diane Holder • ReliabilityFirst  
Christi Klein • ReliabilityFirst  
Marcus Noel • ReliabilityFirst  
Niki Schaefer • ReliabilityFirst  
Jody Tortora • ReliabilityFirst



## **c) 2024-3 Resolution Annual Meeting of Members**



RESOLUTION NO. 2024-03

---

**Resolution for  
Annual Meeting of Members**

---

**WHEREAS**, the Corporation's Bylaws provide that the Corporation shall hold an Annual Meeting of Members in December of each year, or at such other time as specified by the Board of Directors, to elect directors and for other purposes;

**NOW, THEREFORE, BE IT RESOLVED**, that the 2024 Annual Meeting of Members (Annual Meeting) shall be held at 9:00 am on December 5, 2024 in Washington, DC.

**FURTHER RESOLVED**, that the close of business on November 4, 2024 is designated as the record date for the determination of the Members entitled to notice of and the right to vote at the Annual Meeting;

**FURTHER RESOLVED**, that the nominees selected by the Nominating and Governance Committee for the at-large director and any industry sector directors nominated by the sector to be elected at the Annual Meeting shall be submitted to the Members in the notice of the Annual Meeting;

**FURTHER RESOLVED**, that the authorized officers, each acting alone or together with the other, are hereby authorized and directed to transmit a notice of the Annual Meeting and a proxy form to each Member entitled to notice of and the right to vote at the Annual Meeting;

**FURTHER RESOLVED**, that Niki Schaefer and Kristen Senk of the Corporation, or either one of them, with full power of substitution, are designated as proxies to vote for Members at the Annual Meeting;

**FURTHER RESOLVED**, that Niki Schaefer and Kristen Senk of the Corporation, or either one of them, with full power of substitution, are hereby appointed and authorized to tabulate proxies on behalf of the Corporation and to act as the inspectors of election in connection with the Annual Meeting;

**FURTHER RESOLVED**, that all actions heretofore taken by the authorized officers of the Corporation in connection with the subject matter of any of the foregoing resolutions be, and they hereby are, approved, confirmed and ratified in all respects; and

**FINALLY RESOLVED**, that the appropriate officers of the Corporation be and they hereby are authorized and directed to take all actions and execute all such documents as they deem necessary or appropriate to effectuate the foregoing resolutions.

As adopted on this 22<sup>nd</sup> day of August, 2024 by  
the Board of Directors,

Niki Schaefer  
*Vice President, General Counsel & Corporate  
Secretary*

## **e) Proposed 2025 Meeting Dates**



## **ReliabilityFirst Proposed Meeting Dates for 2025** *(all dates are Wednesday-Thursday)*

Request for approval of the following dates for the 2025 ReliabilityFirst Board Directors and Committee meetings.

**1<sup>st</sup> and 2<sup>nd</sup> Quarter**

**April 30 – May 1**

**3<sup>rd</sup> Quarter**

**August 20-21**

**4<sup>th</sup> Quarter and Annual Meeting of Members**

**December 3-4**

# Bio



**Kurtis Minder**  
**CEO and co-founder of GroupSense**

Kurtis Minder is the CEO and co-founder of GroupSense, a leading provider of digital risk solutions. Kurtis built a robust cyber reconnaissance operation protecting some of the largest enterprises and government organizations.

Kurtis has been the lead negotiator at GroupSense for ransomware response cases. He has successfully navigated and negotiated some of the largest ransomware, breach, and data extortion cases worldwide.

In addition to being profiled in The New Yorker for his work, he has been featured in the media across four continents. Kurtis has been called on for cyber thought leadership by CNN, The BBC, CBS, and other TV News. Kurtis has been covered by publications such as Reuters, The Wall Street Journal, The New York Times, Fortune, The Washington Post, and others.

# Bio





**Colleen Sidford**  
**NERC Board of Trustees**

Colleen Sidford Colleen Sidford was elected to the NERC Board of Trustees in February 2019. Ms. Sidford is the chair of the Finance and Audit Committee and serves on the Corporate Governance and Human Resources and Enterprise-wide Risk Committees. She also serves as the international liaison. Ms. Sidford most recently served, from 2003 until 2013, in a series of roles with Ontario Power Generation Inc. (OPG), including vice president and chief investment officer, vice president and treasurer, and assistant treasurer. In those roles, she had responsibilities that included oversight of more than \$30 billion of assets that comprised OPG's Pension Fund, along with the assets of the Nuclear Used Fuel Fund and Nuclear Decommissioning Fund. In her treasury roles, Ms. Sidford's responsibilities included corporate finance, risk management and insurance, and treasury group operations.

Prior to joining OPG, Ms. Sidford founded and operated a financial services consulting company based in Europe, served as an executive with The Molson Companies and with Bank of America, and held a variety of positions with the Bank of Nova Scotia.

Ms. Sidford has substantial service experience in Canada and Europe, including serving on the Boards of Meridian Credit Union, Boilermaker's National Pension Fund, Health and Welfare Benefits Fund, Canadian Scholarship Trust Foundation, and Invesco Canada Ltd. She also provided investment advisory services to CBRE Calderon Capital LLP. Ms. Sidford previously served as the president of Women in Nuclear Canada for two terms and held board positions with European affiliates of Bombardier Inc., the European Mutual Association of Nuclear Insurers, and CUBE Infrastructure Fund.

# Impact Report



# FORWARD TOGETHER.

2023 IMPACT REPORT

# TABLE OF CONTENTS

---

Chairman and CEO Letter.....	3
What We Do.....	4
Our Organization at a Glance.....	5
Our Value.....	6
Our Strategic Plan.....	7
Our Approach to Compliance and Collaboration.....	8
Our Work in Action: Tackling Regional Risks.....	14
Our People.....	18
ReliabilityFirst in Our Communities.....	19
Senior Leadership.....	20
Governance.....	21

# CHAIRMAN AND CEO LETTER

## Two Decades of Progress

2023 marked the twentieth anniversary of the August 14, 2003 blackout. This massive blackout impacted over 50 million people who lost power across Michigan, Ohio, Pennsylvania, New York, and the Province of Ontario, Canada. The outage caused widespread disruption of essential services and highlighted how dependent we are upon reliable and secure electric service.

ReliabilityFirst (RF) was born out of that blackout and the subsequent Energy Policy Act of 2005, which created the Electric Reliability Organization (ERO), from which we have delegated authority to perform our activities. Our mission is to ensure that the electric grid is reliable and secure, not only for today but also for tomorrow. RF serves the public, and our “why” is to do all we can to make sure the bulk power system is as reliable and secure as possible to ensure our safety, our health and welfare, our economy, and our very way of life.

In the years since that blackout, we have learned a tremendous amount about the vulnerabilities of our grid and have worked diligently with our industry partners to address and mitigate these risks. As time goes by, many currently working in our industry, as well as policymakers, may not recall the impact this event had on our economy, nor do many recognize how complex our bulk power system is and the risks it faces.

As these threats evolve, we are evolving with them. First and foremost, we are staying diligent in identifying and removing well-known and well-established threats. With guidance from our Board of Directors, our partnership with NERC, and the tireless work of our staff and bulk power system partners who produce and transport our energy, we are working to ensure we don't drift back on the progress we have made. This report highlights those essential efforts.

Second, we must continue to work proactively to identify, assess, and communicate new and emerging threats, some of which may be currently unknown. It is imperative that RF work with industry to understand and address these risks when they are small and before they are experienced.

Lastly, while we do not seek to influence or create policy, we must continue to work with policymakers to share our knowledge and analysis to assist them in making informed decisions. These policy decisions have far-reaching and long-lasting impacts, and must be made with a complete understanding of the risks and benefits. Much of our policy discussions are directed at the “energy transition.” This transition involves a significant structural change to our bulk power system regarding the supply and consumption of energy resources, and must be managed appropriately to ensure continued reliability. This report is a testament to the hard work that took place across RF in 2023 and a reminder of the progress we have made over the last 20 years. We are immensely proud of the RF team, our ERO counterparts, our partners at NERC, and the diligent efforts of our 300+ bulk power system partners who collaborate across our footprint to bring us reliable, resilient, and life-changing energy resources.

*Sincerely,*



**Antonio Smyth** - Chair



**Tim Gallagher** - President/CEO

# WHAT WE DO

The electric grid is a vital component of our daily lives. It delivers power to our homes, schools, hospitals, and businesses. The electric grid is often unseen, but it plays a crucial role in our economy, national security, and public welfare.



RF is one of six regional organizations that make up the Electric Reliability Organization (ERO) enterprise, which is responsible for ensuring the reliability and security of the North American Bulk Power System. We receive our authority from the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC).

RF works with utility companies to identify and prioritize risks to the electric grid and develop mitigation strategies. We achieve this through education, outreach, sharing of best practices, and monitoring and enforcing the NERC Reliability Standards. In addition, we conduct periodic short and long-term assessments of grid reliability, including analysis of emerging risks.

RF is an objective, independent, expert voice on grid reliability. We use our objective expertise to help state governments and policymakers understand the impacts and issues associated with the transition to a greener grid. Policy decisions are essential to manage risks as we shift from traditional energy sources like coal, nuclear, and natural gas to more renewable sources like solar and wind. We serve as an independent resource to state-level decision-makers to shine a light on the risks and issues

affecting grid reliability and security matters.

Our footprint covers all or portions of Delaware, New Jersey, Pennsylvania, Maryland, Virginia, Illinois, Wisconsin, Indiana, Ohio, Michigan, Kentucky, West Virginia, Tennessee, and the District of Columbia. Our region is situated within the Eastern Interconnection, and we regulate not only utilities but also PJM and MISO, the two regional transmission organizations in our footprint. We work towards our shared mission with NERC and the five other regions, MRO, NPCC, SERC, Texas RE, and WECC.

Our work is interconnected with external stakeholders from other industries, including critical infrastructure like water, gas, communications, federal agencies, law enforcement, and trade associations. We believe that our people are our greatest asset, and their diverse backgrounds, skills, and experiences drive our success and keep the lights on.

# OUR ORGANIZATION AT A GLANCE

## Our Mission:

To serve the public good and support health and safety through preserving and enhancing the reliability, security, and resilience of the grid.

## Our People:

To foster a respectful, collaborative environment where employees can be and feel like the best version of themselves.

## Our Transparency:

To be open and honest about what we are trying to accomplish and why, to foster productive dialogue.

## Our Fairness:

To be reasonable and consistent.

## Our Accountability:

To act with integrity, take pride in our work and responsibility for our actions, and deliver exceptional results.

## Our Creativity:

To encourage and reward innovative ideas and approaches.



Our services are designed to assist our entities in mitigating risks to the bulk power system through compliance and collaboration and include:

- Engineering and System Performance
- Entity Engagement, Training, and Outreach
- Compliance Monitoring and Enforcement
- Operational Analysis and Awareness
- Registration and Certification
- Risk Analysis and Mitigation

# OUR VALUE

RF was created in response to the 2003 blackout, which had a tremendous impact on the northeastern and Great Lakes areas of the United States as well as Ontario, Canada, including lost lives and billions of dollars in business activity. Our reliance on the bulk power system has grown exponentially since then, which is why RF, its regional ERO partners, and NERC's work to keep the grid highly reliable and secure is vital to our communities and our way of life.

## Value Through Compliance and Collaboration

Consider this: the average U.S. household spends an estimated \$1,623 annually on electricity.\* Of that cost, approximately 55 cents per year, or less than a nickel a month, is spent on our collective services. This small investment ensures that when the switch is flipped, the lights will come on, and our grid will remain secure and resilient.

We assess our performance, prioritize activities, plan resources, and create this stakeholder value through our compliance and collaboration efforts that include the following areas of focus:

- **Energy:** Tackling the reliability and resilience challenges of a rapidly changing energy resource mix, the impacts of extreme weather, and the capability to transfer energy when required.
- **Security:** Focusing on physical and cyber security risks.
- **Agility:** Becoming more nimble in risk identification and standards development.
- **Sustainability:** Investing in automation, eliminating single points of failure, and strengthening the ERO's long-term stability and success.

These efforts are supported by our Strategic Plan and through the commitment of our workforce.

THE AVERAGE U.S. HOUSEHOLD  
SPENDS AN ESTIMATED

# \$1,623

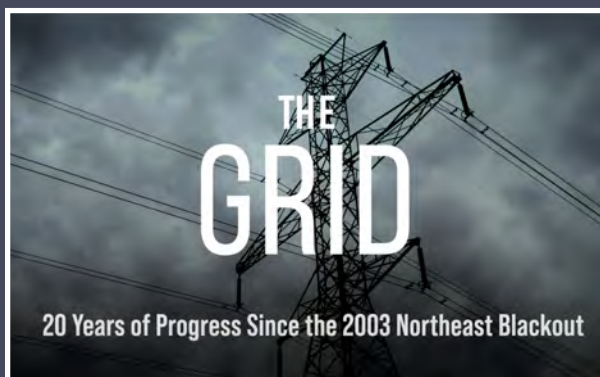
ANNUALLY ON ELECTRICITY

OF THAT COST,  
APPROXIMATELY 55 CENTS  
PER YEAR, OR LESS THAN



\* [https://www.eia.gov/electricity/sales\\_revenue\\_price/](https://www.eia.gov/electricity/sales_revenue_price/)

## THE GRID: 20 YEARS OF PROGRESS SINCE THE 2003 NORTHEAST BLACKOUT



Aug. 14, 2003 marks the 20th anniversary of the 2003 Northeast blackout, which impacted 50 million North Americans across Michigan, Ohio, Pennsylvania, New York and Ontario.

The blackout, the largest ever experienced in North America, prompted the Energy Policy Act of 2005, which created an electric reliability organization (ERO) charged with developing and enforcing mandatory Reliability Standards, assessing current and future reliability trends, analyzing system events, and recommending improved practices. This video linked below was created by RF, NERC and NPCC to reflect on the progress made since then toward a more reliable and resilient electric grid. (<https://youtu.be/sKXVT0V7S0Y>)



# OUR STRATEGIC PLAN

In 2023, we completed the first year of our five-year Strategic Plan. This strategic plan provides a road map for our efforts based on three strategic objectives:



## Be an Excellent Regulator

- Consistently demonstrate accountability, transparency, and efficiency through our operating model.
- Commit resources to collaboration and security.
- Build a deep knowledge of our entities and use it to serve our footprint.

## Cultivate a Highly Engaged, Talented Workforce

- Recruit, retain, and train the right people for the right roles.
- Further enhance and promote diversity, equity, and inclusion.
- Prioritize our positive workplace culture.

## Harness Knowledge to Comprehensively Address Risk

- Quickly deploy communications to mitigate risk based on our data and perspective.
- Develop targeted outreach strategies.
- Enhance our value as an independent resource to broaden our reach.

These objectives inform how we use our authority to achieve our mission. The strategic plan highlights supporting initiatives and notes how we will measure and monitor our performance. Our strategic plan is in direct alignment with our program areas and is intended to bolster the quality and responsiveness of our services.

# OUR APPROACH TO COMPLIANCE AND COLLABORATION

We work to ensure that we are continuously improving in our compliance monitoring and enforcement efforts, and prioritizing our efforts based on risk.

We use Compliance Oversight Plans and Inherent Risk Assessments to guide our compliance monitoring efforts, which are integrated into our Compliance Monitoring and Enforcement Program (CMEP). The RF CMEP is segmented into two groups:

- **Critical Infrastructure Protection (CIP)**
- **Operations and Planning (O&P)**

Our responsibility is to ensure registered entities comply with the NERC Reliability Standards through tools such as:

### **Compliance Auditing:**

An in-depth look at the reliability, security, internal controls, and culture of our entities. The focus is on the mandated NERC Reliability Standards, entity performance, and the inherent risks of entity assets.

### **Self-certifications:**

Monitoring methods in which an entity completes a self-assessment of its compliance activities with applicable NERC Reliability Standards and requirements, and submits substantiating evidence that validates compliance.

### **Spot Checks:**

Tools used to audit smaller scopes focusing on a single risk or two.

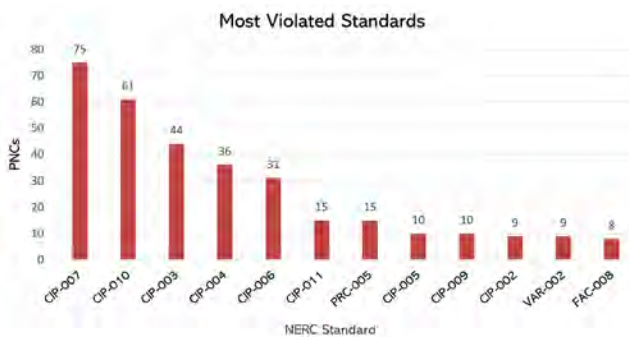


# NONCOMPLIANCE TRENDS AND TAKEAWAYS

RF regularly monitors enforcement data to identify risks, trends, and lessons learned. Throughout 2023, RF shared pertinent data and information through various channels, including webinars, newsletter articles, and board meetings to bring transparency and clarity to the CMEP processes, share lessons learned, and drive continuous improvement. The following overview highlights the most violated standards in 2023.

## Most Violated Standards

Since the implementation of CIP version 5, the number of noncompliances with CIP Standards has consistently outpaced those in the Operations & Planning space, and that trend continued in 2023 as CIP noncompliances comprised approximately 77% of noncompliance intake. The graph below shows the 12 most violated Reliability Standards in 2023 in the RF footprint based on intake.



## CIP Commentary

The sustained high volume of CIP noncompliances is due, in part, to a handful of “high-frequency conduct” CIP requirements (e.g., CIP-007-6 R2 patch management and CIP-010-2 R1 change management), which govern activities that occur often and cover numerous assets and people, leading to more opportunities for noncompliance. Even entities with strong programs will find noncompliances involving patching and change management, but RF encourages entities to continue focusing on the implementation of effective internal controls to drive down the duration and instance counts of issues that do occur. Where this is not the case, the risk will likely be elevated. In CIP-004, we are seeing an increase in issues with managing vendor and contractor access, often involving extended durations where entities do not have strong internal controls to monitor personnel changes.

## Operations & Planning Commentary

PRC-005 (protection system maintenance) and VAR-002 (maintaining voltage schedules) continue to be the most frequently violated Operations and Planning Standards in the RF footprint as they also occupied the top two spots in 2022. From a processing standpoint, 43% of the PRC-005 and VAR-002 noncompliances closed since the start of 2022 were classified as moderate risk. In PRC-005, risk tends to be elevated in cases involving broader proportional misses across an entity’s program with significant durations. RF explored issues relating to VAR-002, including common failure types and suggestions for improvement, in the 2023 Q2 Newsletter.

## Inventory and Self-Reporting

In 2023, RF remained focused on eliminating older open violations. More than 94% of open violations in 2024 Q1 were identified between 2022 and 2024. Consistent with prior years, more than 86% of noncompliances discovered in 2023 were either self-reported or self-logged, showing continued diligence and transparency of entities in identifying and reporting issues.

More than  
**86%**  
of noncompliances  
discovered in  
2023 were either  
self-reported or  
self-logged, showing  
continued diligence and  
transparency of entities  
in identifying and  
reporting issues.

# OUR APPROACH TO COMPLIANCE AND COLLABORATION (CONTINUED)

As a regulator, RF has the authority to impose penalties on entities that violate the NERC Reliability Standards. However, we know well that “you cannot punish your way to excellence.” That is why our collaborative outreach efforts are essential to helping mitigate risks.

RF conducts monthly programs and events to bring registered entities and partners together to share insights and provide learning opportunities, including:

- **Appraisals (Community and Entity)**
- **Assessment Tools**
- **Assist Visits**
- **Committees and Conferences**
- **Newsletters**
- **Research, Reports, and Thought Leadership**
- **Webinars and Workshops**
- **Winterization Visits**

## Appraisals (Community and Entity)

Community Appraisals assess the readiness, preparedness, and resilience of communities in our footprint to withstand long-term disruptions to electrical power and other threats.

Entity Appraisals assess our registered entities' management practices to identify risks, best practices, and opportunities for improvement.

## Assessment Tools

Our Incident Response Preparedness Assessment Tool (IRPAT) evaluates information technology systems' readiness, preparedness, and robustness by performing simulated cyber or physical incident exercises.

Our Cyber Resilience Assessment Tool (CRAT) is a qualitative self-assessment tool that allows entities to evaluate and benchmark their cyber resilience posture and effectiveness.

## Assist Visits

RF pioneered Assist Visits with our entities in 2012 and they are available to address specific program improvements or may pertain to specific approaches for implementing reliability standards.

In 2023

80 Assist Visits

30 50

Cyber Security  
Critical Infrastructure  
Protection (CIP)

Operations &  
Planning  
(O&P)

# OUR APPROACH TO COMPLIANCE AND COLLABORATION (continued)



## Committees and Conferences

RF staff participate in numerous committees across the ERO Enterprise as leaders and subject matter experts. These committees are designed to address risk issues including critical infrastructure protection, transmission planning, protection, generation, standards, and human performance. RF staff also participate and present at industry conferences to share insights, research, and best practices.

## Webinars and Workshops

Throughout the year, RF holds webinars (monthly Tech Talks), workshops, and training programs to bring entities and stakeholders together to discuss critical topics of interest, including protection systems, human performance, winterization, NERC Reliability Standards, & state energy policy.

## Newsletters

RF publishes a monthly newsletter as a value-added channel to share updates on standards, discuss industry issues, communicate collaboration efforts and upcoming events, and share insights from research and work through our various committees and events.

### State Policymakers:

RF also publishes a special monthly newsletter targeted to state

policymakers, to provide pertinent information regarding risks to the bulk power system, such as studies, reports, key regulatory updates, and information on upcoming RF and ERO state outreach events.

## Research, Reports, and Thought Leadership

### Interregional Transfer Capability Study (ITCS):

RF and our regional ERO counterparts are collaborating with NERC to conduct an Interregional Transfer Capability Study (ITCS). The study, directed by the Fiscal Responsibility Act of 2023, will analyze the amount of power that can be moved or transferred reliably from one area of the interconnected transmission systems to another. Transfer capability is a critical measure of addressing energy deficiencies by relying on distant resources, and is vital as the resource mix continues to change.

### Seasonal Resource Reliability Risk Assessment:

RF annually performs seasonal summer and winter reliability assessments to ensure that its footprint has adequate resources to serve anticipated demand.

### Long-Term Reliability Resource Risk Assessment:

RF performs an annual assessment to ensure that its footprint has adequate resources to serve anticipated load demand for the next 10-year period.



# OUR APPROACH TO COMPLIANCE AND COLLABORATION: COLD WEATHER WINTERIZATION VISITS

Recent extreme cold weather events, such as Winter Storm Uri in 2021 and Winter Storm Elliott in 2022, underscore the importance of cold weather preparedness to the grid's reliability and our country's overall safety and well-being.

Winterization visits are a voluntary program where RF staff evaluate the readiness of generating facilities for the upcoming winter season, discuss any concerns, and share best practices to help enhance winter readiness in our region.



*Components wrapped in fire-retardant material to protect susceptible components against freezing during winter months.*



Separate and distinct from mandatory compliance activities, RF staff were able to provide recommendations to plants that address the risk of extremely low temperatures, including:

- Protecting modular platforms with piping, racks, pumps, compressors, or skids that require using temporary coverings in cold weather to prevent freezing.
- Protecting feedwater pumps, heat recovery steam generation (HRSG) drums, level transmitters, flow transmitters, and HRSG header drains located outdoors.
- Protecting the instruments that provide critical operational parameters to the control room.
- Improving how heat tracing cables that provide heat all along their length are serviced or monitored.
- Monitoring performance of high voltage breakers during extreme cold weather conditions for breakers that utilize sulfur hexafluoride (SF6) gas.

The RF team, with their extensive knowledge and experience, are able to provide valuable insights through "positive observations". They also offer practical suggestions on best practices, demonstrating their commitment to improving operational efficiency and safety.

# OUR APPROACH TO COMPLIANCE AND COLLABORATION: STATE OUTREACH

RF and the ERO Enterprise have focused on serving as technical resources for the state's policy-making bodies on risk and reliability issues during this critical time of energy transition.

With experts in power system engineering, control room operations, planning, and cyber and physical security, we are an independent, credible resource for state policymakers to rely upon.

We discuss and testify on important reliability and security issues when needed. Three areas of specific concern when engaging with state policymakers are:

**Addressing the Pace of Change:** As retirements of existing resources occur, how do we address the gaps left behind?

**Understanding Resource Adequacy:** How do we ensure there is enough supply to meet demand? Do we fully understand resource availability and its impact on providing reliable electric service?

**Essential Reliability Services:** Do we understand the technical aspects of grid reliability based on power system dynamics that keep the grid balanced and stable (voltage/frequency/ramping capability)? How do resource losses and introducing new resources with different characteristics impact the BES from a technical perspective?

We work hard to provide sound guidance on risks to the grid, so our policymakers have the information they need to act in our states' best interests.

## Recent State Outreach testimonies included:

**November 2023** – Joint PA/OH Senate in Pennsylvania

**December 2023** – WV Joint House / Senate

**January 2024** – Maryland Senate

**February 2024** – Ohio/Pennsylvania joint testimony in Ohio

**April 2024** – Illinois Senate



# OUR WORK IN ACTION: TACKLING REGIONAL RISKS

As part of our strategic plan to harness knowledge to address risk comprehensively, RF completed its Regional Risk Assessment (RRA), which identified the top risk factors for the region. As the risks to the grid continue to evolve, RF updates its compliance activities, collaboration approaches, and knowledge-sharing programs to help mitigate these risks. Below is a list of the top risks identified in the RRA, along with RF’s compliance, collaboration, and outreach activities that help address these risks.

## ENVIRONMENTAL FACTORS

Environmental factors are likely and impactful, resulting in unplanned power outages. Cold Weather Winterization (CWW) has become increasingly important as the energy resource mix has changed.

### Our Impact - Compliance

- RF monitors and enforces multiple NERC standards related to environmental issues.
- A new Emergency Operating Procedure (EOP) winterization standard (EOP-011-2) requires entities to properly prepare assets for winter weather and an additional winterization standard is also in the works.
- RF continues to monitor vegetation-related standards (FAC-003) to ensure proper controls are in place to mitigate risks posed by vegetation growth.
- RF adopted a new field walk-down approach or “readiness assessment,” working directly with entity field and compliance personnel to address vegetation-related risks.

### Our Impact - Collaboration

- RF offers a Vegetation Management Community of Practice for entities to share best practices.
- RF conducted 23 Cold Weather Winterization (CWW) surveys and 16 entity site visits in 2023 – a 45% increase in CWW site visits from the previous year.
- RF held multiple Tech Talks throughout the year pertaining to environmental issues.
- RF participated in and contributed to the joint FERC, NERC, Regional Entity Staff Report “Inquiry into Bulk-Power System Operations During December 2022 Winter Storm Elliott”. This report resulted in a number of recommendations to reduce risks to reliability posed by cold weather.

## CYBER SECURITY

Critical infrastructure throughout the country is constantly under attack from those wishing to cause disruption and harm. As the electrical grid becomes more complex and technology advances, so does the need for advanced cybersecurity capabilities.

### Our Impact - Compliance

- 86% of noncompliances discovered in 2023 were either self-reported or self-logged, showing continued diligence and transparency from entities in identifying and reporting issues.
- CIP-007-6 (System Security Management and patching) is one of the most frequently violated Standards across the entire ERO. RF continues to monitor this Standard and assess controls regarding system security management and specifically patching. With the rise of malware, spyware, and ransomware, it is critical that all entities with critical assets have controls in place to ensure their patch management process is functioning as intended to reduce security risks.

### Our Impact - Collaboration

- RF created and held the Ohio Security Tabletop, a statewide exercise simulating an attack on critical infrastructure with participants from various industries.
- RF provides independent cyber assessment tools to assist entities, including the Cyber Resilience Assessment Tool (CRAT), the Incident Response Prepared Assessment Tool (IRPAT), and the Insider Threat Preparedness Maturity Assessment Tool (InTP).
- RF conducted a pilot exercise during our February Internal Controls Workshop with the ERO focusing on Electronic Security Perimeters and System Security Management.
- Throughout 2023, RF participated in cybersecurity focused workshops such as GridSecCon and GridEx.



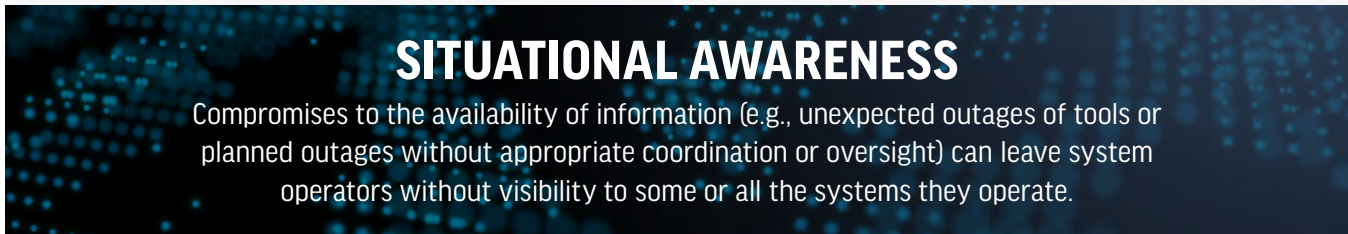
# OUR WORK IN ACTION: TACKLING REGIONAL RISKS (continued)



## CHANGING RESOURCE MIX

Decentralized generation and decarbonization is changing how the grid is planned and operated. Inverter-Based Resources (IBRs), sources of electricity that are asynchronously connected to the grid via an electronic power converter (“inverter”), are being added to the system, replacing conventional synchronous machines.

Our Impact - Compliance	Our Impact - Collaboration
<ul style="list-style-type: none"><li>• RF’s scoping of compliance engagements considers the impact of changing generation resources (such as IBRs).</li><li>• Frequently audited standards in 2023 related to generator performance included PRC-019 “Coordination of Generating Unit or Plant Capabilities, Voltage Regulating Controls, and Protection”; PRC-024 “Generator Performance During Frequency and Voltage Excursions”; CIP-002 “BES Cyber Security Categorization”; and CIP-003 “Security Management Controls”.</li></ul>	<ul style="list-style-type: none"><li>• RF performs extensive state outreach, serving as an expert resource to state legislatures, public utility commissions, and governor’s offices regarding reliability concerns associated with the changing resource mix.</li><li>• RF and NERC publish and promote long-term and seasonal planning assessments alerting stakeholders to resource adequacy risks in the 5-to-10-year horizon.</li><li>• RF is assisting and participating in all aspects of the Interregional Transfer Capability Study directed by Congress in the Fiscal Responsibility Act of 2023.</li></ul>



## SITUATIONAL AWARENESS

Compromises to the availability of information (e.g., unexpected outages of tools or planned outages without appropriate coordination or oversight) can leave system operators without visibility to some or all the systems they operate.

Our Impact - Compliance	Our Impact - Collaboration
<ul style="list-style-type: none"><li>• RF performs compliance oversight, including a focus on TOP-001-5 “Transmission Operations,” to ensure that entity EMS and SCADA systems have the necessary protections in place.</li><li>• TOP-001-5 requires that Real-time Assessments, Operating Plans, and Operational Instructions are monitored to ensure that System Operators have the tools and training needed to study and react to changing system conditions.</li></ul>	<ul style="list-style-type: none"><li>• The ERO published three <a href="#">Lessons Learned documents</a> related to Situational Awareness by monitoring and studying EMS/SCADA outages, to help share risks and mitigations with the industry.</li><li>• RF participated throughout the year in the NERC Event Analysis Subcommittee, and participated in the NERC Monitoring and Situational Awareness Conference.</li></ul>

# OUR WORK IN ACTION: TACKLING REGIONAL RISKS (continued)

## PHYSICAL SECURITY

The protection of assets like substations, transformers, generating facilities, and control centers from threats that may compromise the operation or purpose of those assets.

### Our Impact - Compliance

- RF helps to ensure the security of physical assets by monitoring compliance with NERC Reliability Standards CIP-014 "Physical Security," and CIP-006 "Physical Security of BES Cyber Systems".
- In August of 2023, FERC held a joint [NERC/FERC Physical Security Technical Conference](#) to discuss how regulators and utilities can partner together to strengthen physical security controls.

### Our Impact - Collaboration

- In 2023, RF conducted a security drill for the state of Ohio and began preparations to conduct a security drill for the state of New Jersey in 2024.
- RF has a tabletop tool for entities to self-assess their readiness for and responsiveness to a physical security attack.
- RF offers an Assist Visit program for entities to ask questions and discuss best practices with a subject matter expert.

## MISOPERATIONS

The failure of a protection system to operate as intended exacerbates unplanned transmission outages that are not being monitored or planned.

### Our Impact - Compliance

- PRC-004 "Protection System Misoperation Identification and Correction" was one of the most frequently audited standards in 2023 to address this risk, along with additional PRC standards.
- Misoperations have reduced from approximately 13.6% in 2014 to 7.8% in 2023 (Q1-Q3), a 43% reduction.
- Misoperations related to human performance issues have declined 58% over the last four years.

### Our Impact - Collaboration

- In 2023, the RF Protection Subcommittee and Engineering and System Performance Department hosted their 9th annual Protection System Workshop.
- RF continued to conduct one-on-one meetings with entities, reviewing misoperations data and sharing best practices.
- The RF Protection Subcommittee developed a Misoperations Assessment, identifying industry trends and making recommendations for improvement.

# OUR WORK IN ACTION: TACKLING REGIONAL RISKS (continued)

## MODELING

Modeling and Facility Ratings are crucial to understanding the operating limits of the bulk power system. This risk overlaps with IBR risks based on post-event analysis of events such as the Odessa disturbances in 2021 and 2022.

### Our Impact - Compliance

- RF's compliance monitoring team reviews the MOD (modeling) standards, and the FAC (facility rating) standards to ensure accuracy for operational and planning assessments.
- In 2023, RF continued its Facility Ratings walk-down initiative, where RF staff spent time with registered entities in the field and within substations, verifying equipment and models and discussing change management techniques.

### Our Impact - Collaboration

- RF partnered with NERC to host a Facility Ratings Management webinar focused on change management controls in May 2023.
- RF participates in the annual Planning and Modeling Virtual Seminar with NERC and industry (EPRI/NATF), plus the Acceptable Modeling Workshop Group with the Eastern Interconnection Reliability Assessment Group (ERAG).
- Additional NERC task forces with RF participation such as the System Planning Impacts from DER Working Group (SPIDERWG) have raised awareness to IBR modeling issues.



# OUR PEOPLE

We are more than just a team – we are a community of dedicated professionals committed to ensuring the reliability and security of the electric grid. We have a staff of approximately 100 employees at RF, including a mix of skilled professionals in engineering, auditing, cyber security, law and other specialties, many which have past industry experience in control room operations, planning and other areas. Our employees are passionate about the work they do and their positive impact.

At RF, we strongly encourage personal development. We enable our team members to grow both personally and professionally. We provide ample resources and opportunities to support this growth. We firmly believe that investing in our people is an investment in the future of our organization.

## Diversity, Equity, Inclusion & Belonging (DEIB)

At RF, we believe in promoting DEIB. We understand that our success depends on the unique perspectives, experiences, and skills of our employees, stakeholders, and partners. We are committed to cultivating a culture of belonging where everyone is valued, respected, and empowered to contribute towards our goal of ensuring the reliability, security, and resilience of the electric grid.

RF has taken several actions to improve DEIB in our organization and industry, such as:

- Establishing a council of employees from various departments and levels to provide guidance and oversight on DEIB initiatives.
- Conducting regular employee surveys and focus groups to assess the current state of DEIB.
- Providing DEIB training for all employees and managers to raise awareness and foster inclusive behaviors.
- Participating in external DEIB events and programs, such as the North American Electric Reliability Corporation (NERC) Diversity Forum and the Women in Energy Leadership Forum.
- Aligning DEIB goals with organizational strategy and holding senior leaders accountable for their implementation and outcomes.

## THE RESULTS:

# 31%

Female on Board of Directors

# 46%

Minorities, women, veterans, people with disabilities

# 38%

Women in leadership positions, manager, and above



We are proud of our selection by the Cleveland Plain Dealer as one of the Top Workplaces in Northeast Ohio for 2023.

Greater Cleveland  
Food Bank



**RF**

**RELIABILITYFIRST  
IN OUR COMMUNITIES**



# SENIOR LEADERSHIP

Our leadership team is passionate about ensuring the reliability and security of the Bulk Power System, while hiring and supporting top-caliber employees to support this mission.



**Tim Gallagher**  
*President and Chief Executive Officer*



**Beth Dowdell**  
*Senior Director of Corporate Services and Treasurer*



**Jeff Craigo**  
*Senior Vice President, Reliability & Risk*



**Kristen Senk**  
*Director, Legal and Enforcement*



**Niki Schaefer**  
*Vice President and General Counsel*



**Brian Thiry**  
*Director, Entity Engagement*



**Diane Holder**  
*Vice President, Entity Engagement and Corporate Services*



**Matthew Thomas**  
*Director, Compliance Monitoring*



**Marcus Noel**  
*Vice President and Chief Security Officer*



**Jim Uhrin**  
*Director, Engineering and Reliability Services*

# GOVERNANCE

RF's Board of Directors governs and oversees RF's activities according to the corporation's bylaws and its delegation agreement with NERC. Our board has four committees: Risk and Compliance, Talent and Compensation, Nomination and Governance, and Finance and Audit. RF has a hybrid board structure designed to represent our unique history, diverse footprint and commitment to independence, and deep industry knowledge. Our Board structure was carefully designed to include independent directors along with balanced representation from the diverse entities across our footprint. The Board of Directors and its committees meet regularly, with at least three open meetings a year.

## **Antonio Smyth, Chair**

*Executive Vice President of Grid Solutions and Government Affairs, American Electric Power (AEP)*

## **Nelson Peeler, Vice Chair**

*Senior Vice President of Grid Planning and Integration, Duke Energy*

## **Patrick Cass, Lead Independent Director**

*Former Accounting and Advisory Services Industry Professional*

## **Steven Ambrose**

*Vice President and Chief Information Officer, DTE Energy*

## **Joanna Burkey**

*Former Chief Information Security Officer, Hewlett Packard*

## **Lesley Evancho**

*Chief Human Resources Officer, EQT*

## **Timothy R. Gallagher**

*President and Chief Executive Officer, ReliabilityFirst*

## **Craig Grooms**

*Chief Operating Officer with Ohio's Electric Cooperatives and Buckeye Power*

## **Scott Hipkins**

*Vice President, Cyber Security and CISO, FirstEnergy Corp*

## **Ken Seiler**

*Vice President, System Planning, PJM*

## **Rachel W. Snead**

*Director, Environmental Services, Dominion Energy*

## **Jennifer T. Sterling**

*Vice President, NERC Compliance & Security, Exelon*

## **Joe Trentacosta**

*Senior Vice President and Chief Information Officer (CIO), Southern Maryland Electric Cooperative (SMECO)*

## **Simon Whitelocke**

*Vice President of ITC Holdings Corporation and President of ITC Michigan*



---

3 Summit Park Drive, Suite 600  
Cleveland, OH 44131

216-503-0600 | [www.rfirst.org](http://www.rfirst.org)



## **a) CIP Themes Report**

# 2024 CIP THEMES REPORT

Tom Scanlon, Managing Enforcement Counsel, ReliabilityFirst

August 22, 2024

Canton, OH



# 2024 CIP THEMES REPORT



## Purpose

- Highlight themes and areas for improvement
- Suggest potential resolutions

## Sharing and Collaboration

- Industry-wide data
- ERO Enterprise-wide participation, analyses, and drafting

## Third Edition

- Second edition in 2018

# LATENT VULNERABILITIES

## THE IMPORTANCE OF INTERNAL DETECTIVE CONTROLS

- Long-standing, higher risk issues that evade detection and persist within entities' environments
- Examples in physical security, electronic access, and patching



# INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

## THE NEED TO REVISIT APPROACHES TO CIP-003 R2

- Misunderstanding CIP obligations and security objectives
- Insufficient understanding of cyber environments and struggling to effectively manage electronic access
- Struggling to implement effective TCA plans



# SHORTAGES OF LABOR AND SKILLSETS

## CHALLENGES IN WORKFORCE AND SUCCESSION PLANNING

- Challenging threat landscape coupled with reported labor shortage
- Issues transitioning work or managing organizational complexities
- Key personnel



# PERFORMANCE DRIFT

PHYSICAL SECURITY ISSUES AS MARKERS OF PERFORMANCE DRIFT AND APATHY

- Increased failure in physical security programs when disciplined execution becomes inconvenient or uncomfortable
- Bypassing security controls, relying on assumptions, propping doors, leaving doors and gates open, and sharing badges and PINs



# NEXT STEPS

- Webinars, conferences, workshops
- Private briefings
- Supplemental outreach





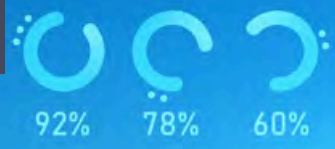
# QUESTIONS & ANSWERS

Tom Scanlon

[tom.scanlon@rfirst.org](mailto:tom.scanlon@rfirst.org)



## **b) 2024-CIP-Themes-and-Lessons-Learned**



# CRITICAL INFRASTRUCTURE PROTECTION

## THEMES AND LESSONS LEARNED

MITIGATING RISKS BEHIND THE CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

2024





# PREAMBLE AND LIMITATION OF PURPOSE

Through their compliance monitoring, enforcement, outreach, and other activities, the North American Electric Reliability Corporation (NERC), ReliabilityFirst Corporation (RF), Southeast Reliability Corporation (SERC), Western Electricity Coordinating Council (WECC), Midwest Reliability Organization (MRO), Texas Reliability Entity (Texas RE), and the Northeast Power Coordinating Council (NPCC) (collectively, the ERO Enterprise) have identified risk themes that have made it difficult for some entities to mitigate risks associated with the NERC Critical Infrastructure Protection (CIP) Reliability Standards.[1] The purpose of this report is to communicate these themes (and possible resolutions to them) so that we can work together to continuously assure the reliability of the Bulk Electric System (BES). While there are many discrete valuable lessons learned published by the ERO Enterprise to promote strong CIP performance, this report is intended to identify and share broader themes.

The suggestions for possible resolutions in this report are not, and should not be construed as, mandatory directives to industry. Rather, most of these possible resolutions are merely approaches that have been successful for certain entities. However, these possible resolutions may not be the best approach for every entity because the impact of the resolutions is largely driven by variables such as an entity's size, structure, workforce, technology, culture, and other factors.

[1] The power industry is subject to mandatory Reliability Standards for CIP. The entities discussed in this report have worked with, or are working with, the ERO Enterprise to resolve and mitigate any noncompliance with the CIP Reliability Standards.



# TABLE OF CONTENTS

---

04

## EXECUTIVE SUMMARY

05



## LATENT VULNERABILITIES

The importance of internal detective controls

09



## INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

The need to revisit approaches to CIP-003 R2

13



## SHORTAGES OF LABOR AND SKILLSETS

Challenges in workforce and succession planning

16



## PERFORMANCE DRIFT

Physical security issues as markers of performance drift and apathy

20

## CONCLUSION



# EXECUTIVE SUMMARY

The ERO Enterprise pursues its mission of ensuring the effective and efficient reduction of risks to the reliability and security of the Bulk Power System. Through targeted engagement and outreach, the ERO Enterprise communicates themes, lessons learned, and best practices throughout each year.

It is also important for the ERO Enterprise to step back, evaluate broader themes over a longer period, and share those themes with industry, along with possible resolutions. To that end, this report is the third installment of “CIP Themes and Lessons Learned,” with prior iterations having been released in 2015 and 2018. While industry excels at many aspects of cyber security, the intention of this report is to outline areas for improvement with the goal of driving continued progress toward our shared mission of ensuring a reliable power system.

In this report, the ERO Enterprise strives to balance the importance of protecting entity information and security while still providing actionable examples of common or significant issues. Accordingly, the ERO Enterprise included high level fact patterns from open and closed cases in this report while at the same time avoiding the inclusion of information that, if released publicly, could jeopardize the security of the BES or be useful in planning an attack on energy infrastructure.

The four main themes the ERO Enterprise has identified are:

- Latent vulnerabilities;
- Insufficient commitment to low impact CIP programs;
- Shortages of labor and skillsets; and
- Performance drift.

Each of these themes is explored in more detail on the following pages, including suggestions to better address underlying issues and mitigate cyber security risks to the BES.

# LATENT VULNERABILITIES

*The importance of internal detective controls*

THEME  
1

## Observations

In the years since the implementation of CIP version 5, the ERO Enterprise has observed many entities with medium or high impact BES Cyber Systems mature their approach to cyber security and CIP compliance, including notable advancements in internal controls programs. As a result, the nature of noteworthy CIP violations has fundamentally changed.

**Latent Vulnerabilities**  
Long-standing, higher risk issues that evade detection and persist within entities' environments.

For instance, there are far fewer examples of entities running medium or high impact CIP programs with widespread, programmatic issues.[2] These types of cyber security "fall downs" were relatively common during, and in the years following, the implementation of CIP version 5. They were hallmarked by significant violations across several areas [3] with overlapping durations and root causes, many of which could be tied back to themes outlined in prior iterations of this report (i.e., organizational silos, disassociation between compliance and security, lack of awareness, and inadequate tools or ineffective use of tools).

While these broad-spectrum misses were not acceptable, growing pains were expected as large entities were trying to implement complex security protocols across multiple business units (and sometimes affiliates) and many assets. Industry responded to these issues and focused on building sustainable, scalable CIP programs with improved internal controls. The result has been a decline in widespread, programmatic failures, and entities have made strides in (a) preventing widespread issues before they start and (b) developing strong, routine detective controls to quickly identify most issues that do arise.

Even though there has been a decline in programmatic failures, the ERO Enterprise is still seeing long-standing, higher risk issues that evade detection and persist within entities' environments.[4] For the purposes of this report, the ERO Enterprise is going to refer to these issues as "latent vulnerabilities."

[2] As outlined later in this report, some of these broader issues are still occurring at entities with low impact programs.

[3] For example, access management and revocation, electronic security perimeters, interactive remote access, physical security plans, ports and services, security patch management, security event monitoring, configuration change management, configuration monitoring, vulnerability assessments, transient cyber asset and removable media management, and information protection.

[4] On a positive note, these violations have been more isolated in nature. But the point of this theme is to highlight the negative aspects of these cases in an effort to drive continuous improvement and further eradicate cyber security risks to the BES.

# LATENT VULNERABILITIES

## Examples of Latent Vulnerabilities

In a case involving a physical security issue, an entity failed to monitor physical access points to substations. The entity implemented alarms and alerts to monitor for unauthorized access, which created a false sense of security that monitoring was occurring, but failed to recognize that configurations utilized during construction of the substations effectively eliminated the alarms and alerts. After evading detection for nearly three years, the vulnerability (i.e., lack of monitoring of physical access points) was finally discovered in preparation for an internal audit.



There are multiple examples of significant failures related to managing electronic access:

- An entity discovered that thousands of unauthorized users had improper access to BES Cyber System Information (BCSI) for nearly six years due to an inherited and overlooked configuration. The issue was discovered by happenstance. While helping a successor navigate files, a transferred employee realized that she had remaining unauthorized access to files, and further investigation uncovered the full extent of the issue. A quarterly detective control (access reviews) consistently failed to identify the issue because the user group/configuration causing the improper access capabilities was not included in the test population and access lists were not being pulled from the best source.
- More than 100 administrators had unauthorized access to BCSi repositories for over eight years. The issue dated back to the effective date of CIP version 5, and the entity failed to consider the type of access at issue when designing and executing its access management procedures and controls. The issue was discovered by happenstance when a subject matter expert completing other work noticed the potential error.
- Multiple user groups had unauthorized and unmanaged backend access to BCSi repositories due to an entity's lack of understanding of the technical architecture of its systems. The issues spanned several years and were discovered only when the entity was working on a new initiative.



# LATENT VULNERABILITIES

- An entity failed to identify and manage four shared accounts, leading to the failure of Energy Management System (EMS) hosts and a loss of Supervisory Control and Data Acquisition (SCADA) visibility. The loss of visibility was attributed to two of the accounts automatically locking out following password expiration. The issue dated back to the effective date of CIP version 5 and was not discovered until the system outage investigation. An extent of condition review uncovered issues with additional shared accounts, and the violation spanned nearly three years.

A final representative case involves a patching issue discovered during a compliance audit conducted by a Regional Entity. An entity failed to accurately identify a patch source for a critical system application. The entity had identified a legitimate, albeit incorrect, patch source with a name very similar to the correct patch source, which contributed to the delayed discovery of the issue. As a result of relying on an incorrect patch source, security patches for the critical system application were not evaluated or applied for over three years.

Many entities dealing with such latent vulnerabilities have mature CIP programs with well-designed and strong internal controls, and the existence of these issues does not necessarily prove otherwise. But it does suggest that entities should consider utilizing additional or different tools or methods to identify latent vulnerabilities that may exist in their environments. As demonstrated in the examples above, failing to do so may allow significant issues to persist unidentified and uncorrected until: (a) someone accidentally discovers and reports them; (b) audit activities uncover them; or (c) a latent vulnerability reveals itself or is leveraged adversely, thereby causing operational issues.

## Suggestions to Address Latent Vulnerabilities

To address latent vulnerabilities, the ERO Enterprise encourages entities to revisit their approach to detective controls. Entities should consider, without limitation, whether they are:

1. Dedicating sufficient resources to the development, implementation, testing, and execution of detective controls.
2. Conducting regular and sufficient testing of detective controls. Considering some of the examples above, testing to ensure that alarms and alerts from the substations functioned from end-to-end could have uncovered that issue much sooner. In some of the electronic access cases, access reviews failed to uncover the issues because the entities were using insufficient lists to compare access to authorization records. As part of testing controls, entities should ask whether

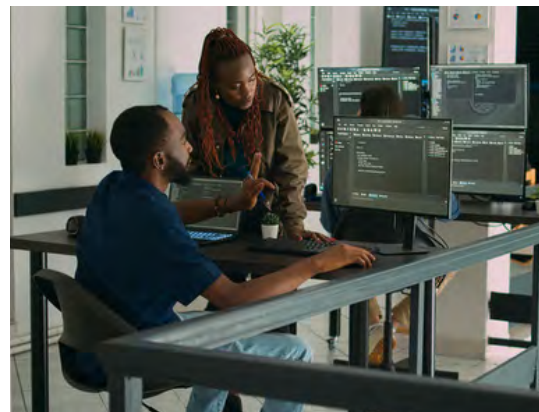
# LATENT VULNERABILITIES

the detective control is relying on the best evidence and source records, as opposed to summaries, manually populated reports, or other records that carry a risk of being incomplete or inaccurate.

3. Periodically scrutinizing the design of existing detective controls and contemplating scenarios that those controls may not address.
4. Conducting appropriate internal audits and assessments, and preferably not just in the months leading up to a compliance audit conducted by a Regional Entity as (a) there may be years between such engagements, (b) external compliance audits are sample-driven and may not uncover latent vulnerabilities, and (c) entities should be more proactive in their pursuit of identifying and correcting cyber security risk.

The ERO Enterprise recognizes that resource constraints and practical realities prevent in-depth, detailed internal audits of every aspect of a medium or high impact CIP program, but they should not prevent entities from thinking critically, ranking the biggest risks to their environment based on several factors, and periodically and heavily scrutinizing those areas.

In addition to formal internal audits, entities could train internal subject matter experts to periodically search for latent vulnerabilities. At registered entities, the point person responsible for CIP-004 detective controls may not be a technical expert familiar with implementing, configuring, and provisioning access to BCSI. In this scenario, it might make sense to leverage an internal expert to conduct a review of configurations and access privileges and search for latent vulnerabilities.



Even if the hypothetical CIP-004 point person is a technical expert, bringing in a fresh set of eyes to conduct a peer review may be optimal to avoid a situation where a person is so close to something that they miss an obvious issue.

5. Leveraging and acting on internal vulnerability assessments, third party security assessments, penetration testing, and other activities designed to catch and correct latent vulnerabilities before they are exploited.

# INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

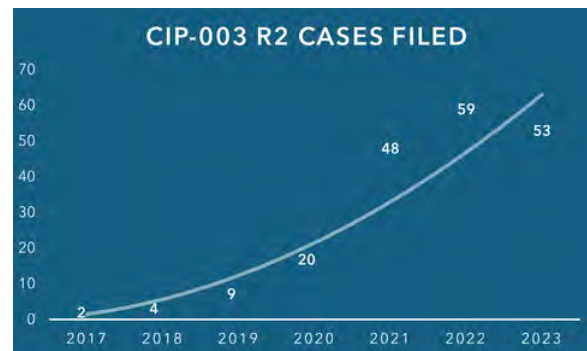
*The need to revisit approaches to CIP-003 R2*

THEME  
**2**

## Observations

In a vacuum, individual assets containing low impact BES Cyber Systems (sometimes referred to herein as “low impact assets”) may not pose a significant risk to the overall BES. Nevertheless, compromise of such assets could create localized issues, and an individual low impact asset could (a) serve as a channel to attack other assets or (b) be used to conduct reconnaissance. And the potential risk to the BES multiplies in scenarios where several low impact assets are compromised in a coordinated attack.

CIP-003 R2 contains the majority of low impact cyber security requirements with a focus on cyber security awareness, physical security controls, electronic access controls, cyber security incident response, Transient Cyber Asset (TCA) and removable media malicious code risk mitigation, and now as part of CIP-003-9, vendor electronic remote access security controls.[5] Between 2017 and 2023, the ERO Enterprise processed a steadily increasing volume of noncompliances with CIP-003 R2.



The ERO Enterprise does not expect this trend to reverse in the next few years because: (a) CIP-003 R2 violation intake—including compliance monitoring findings—and inventory remain at high levels; (b) the ERO Enterprise anticipates that the number of entities with low impact assets will continue to grow (e.g., ongoing efforts relating to registration of inverter-based resources); and (c) new and future requirements are raising the bar as it relates to low impact security obligations (e.g., the above-referenced incorporation of vendor electronic remote access security controls into CIP-003-9).

The ERO Enterprise has observed concerning trends in these violations. Nearly two-thirds of the violations involve examples of low impact entities that:

- misunderstand CIP obligations and security objectives;
- have an insufficient understanding of their cyber environment and struggle to effectively manage electronic access (i.e., inbound/outbound access); or
- struggle to implement effective TCA plans.

[5] In addition, CIP-012 requires all entities, including those running only low impact programs, to protect certain communications between Control Centers.

# INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

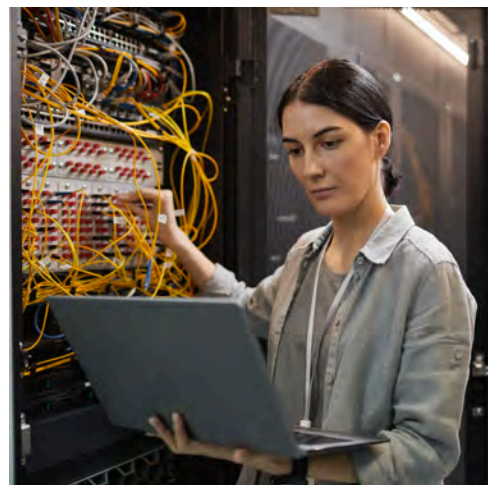
Some individual cases involve a blend of these issues, as detailed in the next section, but a majority of the failures involve the second trend (insufficient understanding of cyber environment and struggling to manage electronic access).

## Examples of Insufficient Commitment to Low Impact Programs

As it relates to the first trend (misunderstanding of CIP obligations and security objectives), there are two main types of cases. First, there are many examples of improper or limited training of personnel responsible for completing requirements (e.g., staff misinterpreting requirements, lack of understanding of expectations, and lack of familiarity with documented policies, processes, and procedures). Second, there are many examples of low impact sites experiencing changeover in ownership, leadership, operations management, or compliance oversight (sometimes successive and frequent changeover at one site). In this second type of case, the ERO Enterprise has seen an increased frequency of entities ignoring, or taking a complacent approach to, the security objectives of CIP-003 R2.

The second trend involves two failures that often go hand-in-hand (insufficient understanding of cyber environment and struggling to manage electronic access). Certainly, it can be difficult to manage electronic access in and out of an environment without an adequate understanding of what is in that environment and how it is configured. There are many examples of entities: (a) with incomplete or inaccurate network diagrams; or (b) failing to identify, understand, or secure potential connections in and out of the environment. Many of these scenarios involve an added layer of coordination with third party vendors.

Cases involving the third trend (struggling to implement effective TCA plans) often have some overlap with the first trend (misunderstanding CIP obligations and security objectives). In many of these cases, the entity has a documented TCA and removable media malicious code risk mitigation plan but little or no evidence that staff are observing and executing the plan. For example, one entity's process required completion of a form and the capture of evidence demonstrating that a TCA had been scanned for malicious code prior to each use. Even though the entity confirmed that TCAs had been used, they could



# INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

not locate a single completed form and had no evidence of scanning for malicious code prior to use. Another entity could not identify how many TCAs were in use, let alone provide evidence showing management of those TCAs to reduce the risk of introducing malicious code in the environment.

## Suggestions to Address Insufficient Commitment to Low Impact Programs

The ERO Enterprise has seen entities run their own low impact programs, rely exclusively on third parties, or use a hybrid approach. As an added layer and regardless of approach, many of these entities rely on vendors to varying degrees to handle specific activities within their program. The ERO Enterprise is not implying that any one approach is better than the others. The suggestions below are relevant to all low impact program types.

This theme highlights the need for improvements in attention to detail, planning, and execution to achieve security objectives at low impact sites. Entities with low impact BES Cyber Systems should consider revisiting their approach to achieving security objectives, evaluate whether personnel responsible for executing the program understand expectations and how to meet those security objectives, and ensure that personnel understand their cyber environment. Similarly, entities purchasing (i.e., buyers) or otherwise taking over the management of (i.e., operations and management or compliance management companies) existing low impact sites should engage in the same evaluation.

As part of this evaluation, entities should:

1. Understand what technology makes the facility work (what they own, what technology is in their environment, and what is running, or capable of running, their facility). The ERO Enterprise acknowledges that CIP-002.5.1a R1, P1.3 states that “a discrete list of low impact BES Cyber Systems is not required[,]” and a note in the current version of CIP-003 R2 provides that “[a]n inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.” But these statements do not excuse entities’ obligations to protect those systems and assets under CIP-003 R2. Indeed, it may be very difficult to achieve the security objectives of CIP-003 R2 without such inventories and lists, so entities should strongly consider developing and maintaining them.
2. Understand how that technology is configured and how they are protecting it.

# INSUFFICIENT COMMITMENT TO LOW IMPACT PROGRAMS

3. Ensure that their program includes sufficient and consistent training and education on security practices and objectives.
4. Ensure that channels of communication between staff and leadership are open for the identification and mitigation of security vulnerabilities.
5. Ensure that their program clearly delineates roles and responsibilities at the facility and operations level (be sure to account for third party responsibilities, if any).
6. Identify ways to regularly verify execution of the program to achieve desired results.

Throughout this process, entities should identify areas for improvement and strive to implement a program that focuses on security posture and security objectives as opposed to treating CIP-003 compliance as a set of “check the box” activities.

## Entities with Medium or High Impact BES Cyber Systems

Up to this point, this theme has predominantly been written from the perspective of an entity that has low impact BES Cyber Systems only. But that is not to say that entities that also have, or traditionally had, medium or high impact BES Cyber Systems haven’t encountered issues managing low impact BES Cyber Systems. In fact, there is one sub-theme that entities in this category should be aware of: staff may be unfamiliar with low impact obligations and expectations.

As examples at low impact sites, the ERO Enterprise has seen experienced staff: (a) remotely unlocking doors for unauthorized individuals; (b) neglecting to secure doors and manage keys; and (c) generally failing to identify a need to create or apply security plans to new sites or sites transitioning from medium/high to low impact.

Root causes in these cases often point to ineffective training and lack of direction or guidance, which can result in staff treating low impact sites as functionally out of scope for NERC CIP purposes, which in turn can increase the frequency of less-than-desirable security decisions. Entities in this category may be able to adapt many of their existing policies, processes, procedures, and practices to encompass their low impact BES Cyber Systems, and the ERO Enterprise encourages them to reengage staff executing responsibilities for low impact BES Cyber Systems to ensure expectations are clear.

# SHORTAGES OF LABOR AND SKILLSETS

*Challenges in workforce and succession planning*

THEME  
**3**

## Observations

The gap between the number of cyber security workers needed and the number available has increased 12.6% year over year.

[6] This significant increase represents a growing unmet demand for cyber security labor. And this is occurring at a time when (a) 70% of organizations in the energy/power/utilities industry report a shortage of cyber security staff,[7] (b) 79% of organizations in this industry view the current threat landscape as the most challenging it has been in the past five years,[8] and (c) there have been reports of substantial skills gaps in the cyber security workforce.[9]

Tying this back to the CIP Reliability Standards, the ERO Enterprise often sees noncompliances that result, at least in part, from entities losing skilled labor (e.g., voluntary separation for new employment, retirement, etc.) and failing to successfully transition the underlying job responsibilities to new or existing staff (e.g., succession planning). For example, one registered entity has requested lengthy mitigation extensions in several cases due to issues restructuring and reassigning work following employee departures.

Sometimes the failure is attributable to knowledge transfer issues, and other times it is attributable to entities struggling to find knowledgeable and experienced individuals who are capable of adapting to the evolving electric and cyber security industries.

At the same time, the ERO Enterprise is seeing entities struggle to provide new and existing staff with the tools and resources necessary to strengthen their understanding of the nuanced issues and difficulties that arise in this space. Over time, the issues above can limit an entity's ability to (a) design and operate successful and sustainable security and compliance programs and (b) prevent, detect, and respond to cyberattacks.



[6] ISC2 Cybersecurity Workforce Study, p. 5 (2023)

[7] ISC2 Cybersecurity Workforce Study, p. 18 (2023)

[8] ISC2 Cybersecurity Workforce Study, p. 66 (2023)

[9] ISC2 Cybersecurity Workforce Study, p. 20 (2023)



# SHORTAGES OF LABOR AND SKILLSETS

Large entities are complex, with hundreds of individual technology systems, cloud services, suppliers, processes, and interfaces making the identification of, and training on, critical skillsets essential. This complexity makes it extremely difficult to gauge what tools, resources, and staffing are needed to support a large entity's program or specific areas of the program. Defining roles in large organizations is necessary and essential to ensuring there are personnel assigned and aware of their responsibilities. In large organizations, there are often several individuals or groups touching the same set of assets, and clearly defining roles assists in eliminating uncertainty and creating accountability. In one case, an entity failed to clearly define roles and responsibilities among separate information technology groups and lacked an overarching control to manage organizational changes. This resulted in failures to (a) execute password changes for newly-commissioned devices, (b) fully inventory all known default or generic accounts, and (c) identify individuals authorized to access shared accounts.

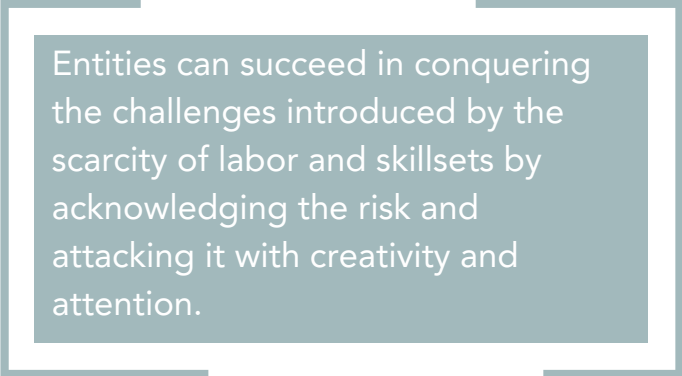
Small entities are also complex and often working with limited resources and tools, which can create barriers to effectively maintaining their own program, especially without third party assistance. Often, staff of small entities must gain expertise in multiple technology systems due to limited resources. The loss of a single employee can be significantly more disruptive to a small entity's security planning and posture because that single individual may represent a larger proportion of the entity's overall cyber security and compliance workforce. Small entities often rely on fewer employees, which can make any loss more impactful.



## Suggestions to Address Shortages of Labor and Skillsets

Entities should consider the following suggestions as they navigate issues relating to shortages of labor and skillsets:

1. Sources of skilled staff include existing employees with the required skills and experience, hiring new staff with the needed skills and experience, or training and mentoring new or existing staff to gain the desired skills and experience.



Entities can succeed in conquering the challenges introduced by the scarcity of labor and skillsets by acknowledging the risk and attacking it with creativity and attention.

The industry as a whole will continue dealing with the departure of a large and skilled generation from the workforce. While these experienced individuals are still in the workforce, entities should take the opportunity to hire new staff and use their experienced staff to educate and train their successors.





# SHORTAGES OF LABOR AND SKILLSETS

Existing knowledge must be shared with and expanded upon by new employees. As availability of skilled and experienced staff remains at low levels, training and mentoring may be the best option for increasing or maintaining appropriate levels of skilled staff.

2. Entities might have to reassess their human resources approach to navigate an increasingly competitive field to induce employees to join and stay at an entity. They may also need to rework and reimagine their recruiting efforts, from colleges and high schools to job fairs, to build awareness around the importance of the energy sector and the opportunity for security professionals to make an impact on such an essential and foundational service.

3. When implementing new processes or internal controls, entities should ensure adequate resources to execute the process or internal control without overly tasking existing staff. They should develop processes or internal controls in coordination with the staff responsible for executing them. Further, they should ensure that said staff have a way to share feedback on unmanageable processes or internal controls to management (before such unmanageable processes or internal controls lead to failure or burnout).

4. When considering new vendor technology, entities should take advantage of and ensure that responsible personnel engage in demonstrations and training offered by the vendor prior to implementation.

5. Entities should implement succession plans for staff who support technology solutions, processes, or internal controls. The departure of single employees should not lead to process or internal control failures or an inability to manage a technological solution. Succession planning is critically important for staff with unique responsibilities. Entities should: (a) strive to identify unique technical tasks and prioritize those tasks based upon risk; (b) document those tasks thoroughly (e.g., procedures, work instructions, job aids); and (c) implement short- and long-term plans to handle these tasks in the event of primary staff departure.

6. Where possible, entities should create process, internal control, and technology commonalities between departments, business units, or affiliates as it can increase the available staff who may be able to address workforce and skillset shortage issues.

7. The ERO Enterprise is working hard to help highlight the critical skillsets needed and assist industry in continuing to develop and maintain these critical skillsets across their workforce. Many different tools and resources are available to help entities optimize their security and compliance cultures, such as training, workshops, seminars, webinars, e-learning modules, and articles on best practices and lessons learned regarding emerging cyber security risks.

# PERFORMANCE DRIFT

*Physical security issues as markers of performance drift and apathy*

## Observations

Physical security has long been a focal point for the ERO Enterprise, originating with NERC Urgent Action Cyber Security Standards 1205 (Physical Security Perimeter), 1206 (Physical Security Controls), and 1208 (Monitoring Physical Access) and continuing today through CIP-006-6 (Physical Security of BES Cyber Systems),<sup>[10]</sup> CIP-014-3 (Physical Security),<sup>[11]</sup> and CIP-003-9 R2, Attachment 1, Section 2 (Physical Security Controls).<sup>[12]</sup> Protecting grid assets from physical breach, misuse, and damage is a long-standing and continuous responsibility. But even where there are time-honored and well-communicated expectations, strong programs can slip and decline due to a variety of factors. This theme highlights examples of apathy, circumvention, complacency, inattentiveness, and other types of “performance drift” in physical security programs at entities of every size and type.

One of the many challenges of executing a physical security program is managing tasks that require repetitive behavior over significant periods of time, as there is increased potential for personnel to lose focus on the performance of an individual act or forget the importance of the act itself. Acknowledging this challenge does not authorize process adherence failures, especially when the stakes are high (i.e., poor decisions in NERC-scoped physical security programs can endanger the reliable and secure operation of the BES). The ERO Enterprise has seen increased failure with these repetitive behaviors when disciplined execution becomes inconvenient or uncomfortable.

People often conceive of the BES as a collection of wires, breakers, switches, and turbines. The BES is all of that, but it is also a tremendously intricate system operated by thousands of human beings. Human beings rely on assumptions and frequently operate with social norms, or commonly shared manners, one even being holding the door for others. Of course, in the context of physically protecting low, medium, and high impact BES Cyber Systems, certain assumptions and social norms must be set aside.

[10] CIP-006-6 applies in medium and high impact programs.

[11] CIP-014-3 applies in medium and high impact programs.

[12] CIP-003-9 R2, Attachment 1, Section 2 applies in low impact programs.

# PERFORMANCE DRIFT

## Examples of Performance Drift

The ERO Enterprise has observed entity staff letting individuals into secure areas when those individuals forgot (or never or no longer had) credentials. In multiple instances, an employee who was running late to a shift, without their badge, was able to talk their way through multiple barriers and into a Physical Security Perimeter (PSP). Similarly, individuals returning from leave had their credentials deactivated while on leave, but they were let in regardless after speaking with a security guard who failed to follow security protocols.

There are related cases involving access revocations due to expired background checks or incomplete annual training. In one case, staff witnessed an individual unsuccessfully attempting to badge in and assumed there must have been a technical issue with the badge reader or door; therefore, they opened the door or lent a badge to the individual when, in reality, a security control was functioning as intended to prohibit said access.



Staff have also allowed unauthorized and unknown individuals into secure areas for reasons that can only be described as “they seemed like they were supposed to be there.” Examples here include: (a) allowing a truck to enter and roam a site for over a half hour because it was believed to be an authorized delivery truck; and (b) allowing an unknown individual into a secure area because he was dressed in work coveralls and claimed to be with a vendor. There are more examples of impermissibly propping doors, ignoring alarms, allowing visitors to roam freely, accidentally leaving doors and gates open, sharing badges and personal identification numbers (PINS), and engaging in other poor security practices.

Even worse, there are cases of intentional circumvention and weakening of security controls. In one case, a long-tenured contractor became increasingly frustrated waiting for an escort to begin work in a secure area, so the contractor used available tools to leverage the door open to the area. The contractor was familiar with the importance of access restrictions and the need for escorting within the facility but felt comfortable enough to force entry due to a slight delay in escort availability. This sort of attitude around physical security suggests that culture-driven performance drift could be on the rise.

# PERFORMANCE DRIFT

## Suggestions to Address Performance Drift

To some extent, individuals performing physical security tasks appear to have lost sight of the purpose of access controls and fall into the trap of viewing them as impediments to their role. Some of the failures described above can seem understandable, and maybe even innocuous, but when it comes to the security of the BES, they are unacceptable. It is this sort of complacency and performance drift that will lead to an entity letting the wrong person in on the wrong day with potentially dire consequences. The physical security threat level remains high. As set forth in the E-ISAC 2023 End-of-Year Report, there were “more than 2,800 physical security incidents shared with E-ISAC [in 2023.]”[13]

With elements of social engineering and human error present in most cyber security incidents, the ERO Enterprise encourages entities to refocus on (a) eliminating poor physical security practices and (b) driving discipline in physical security programs. Ideally, entities are not fostering an environment where people are substituting individual judgment calls in place of security protocols.

Given the examples above, it is not difficult to imagine a scenario in which a terminated individual or someone posing as an employee or contractor attempts to exploit human instincts, including the proclivity for blind trust, to access and harm the BES.

This theme underscores that even the oldest and most fundamental security practices in the CIP space require organizational attention. An entity can have cutting edge tools and well-conceived physical security policies yet still experience performance drift.

Ideally, entities are not fostering an environment where people are substituting individual judgment calls in place of security protocols.

To combat performance drift, the ERO Enterprise recommends that entities consider:

1. Testing their organization for potential performance drift on the physical security side. Consider periodic physical penetration testing. Communicate anonymized testing results to staff where failures are identified to create awareness of how simple acts and situations can be leveraged by a bad actor.

[13] Electricity Information Sharing and Analysis Center (E-ISAC) 2023 End-of-Year Report, p. 4 (2023) (<https://www.nerc.com/pa/C/ESISAC/Documents/2023%20E-ISAC%20End-of-Year%20Report.pdf>).



# PERFORMANCE DRIFT

A security program with continuous internal skepticism is necessary to fight the risk of performance drift. Indeed, the need for skepticism in physical security has only been heightened as remote work and turnover have increased, resulting in staff becoming increasingly unfamiliar with colleagues and other departments.

2. Emphasizing and reinforcing through training and other means why process adherence and individual acts matter. Sometimes the execution of an act can become mindless, and the purpose of an act can become lost. It is imperative to highlight real-world examples of the importance of process adherence in physical security. CIP-004-7 R1, CIP-004-7 R2, and CIP-003-9 R2, Attachment 1, Section 1[14] training and awareness activities provide outstanding opportunities for entities to refresh employees in this area.

3. Constructing incentive programs aligned with corporate values to both promote process adherence and whistleblowing when processes are ignored.

[14] CIP-004-7 applies in medium and high impact programs; CIP-003-9 applies in low impact programs.



# CONCLUSION



Cyber security is an ongoing process, and there is always room for improvement. The ERO Enterprise hopes that by shining a light on the topics outlined herein, entities will continue the conversations within their organizations and with their peers and will reach out to staff at the Regional Entities for more tailored conversations regarding entity-specific questions and issues.



# Financial

# FINANCIAL UPDATE

Beth Dowdell, Sr. Director, Corporate Services

August 22, 2024 Canton, OH





# 2024 SECOND QUARTER FINANCIALS

- As of June 30th
  - \$852K (5.4%) Under budget
  - Key variances
    - Funding \$157K ↑
    - Personnel Expenses \$364K ↓
    - Meeting Expenses \$75K ↓
    - Operating Expenses \$268K ↓

# YEAR END PROJECTIONS

- Estimating as of 12/31/24
  - Projecting to be ~\$293K (1%) under budget by year end
  - Key variances
    - Funding \$251K ↑
    - Personnel Expenses \$304K ↓
    - Meeting Expenses \$11K ↑
    - Operating Expenses At Budget

# QUESTIONS & ANSWERS



# Security

# 2024 Q2 SECURITY UPDATE

Marcus Noel, Chief Security Officer

August 22, 2024

Canton, Ohio



# AGENDA

---

SECURITY RISK REGISTER OVERHAUL

THREATS IN THE WILD

- CROWDSTRIKE
- RUSSIA/UKRAINE GPS IMPACT

# SECURITY RISK REGISTER OVERHAUL



**RELIABILITY FIRST**

# LEGACY SECURITY RISK REGISTER

Risk Statement	Likelihood (1-5)	Impact (1-5)	Reputation (1-5)	Inherent Risk	Control Effectiveness	Residual Risk
Entity non-public information RF is responsible for is made available on the Internet and the public is aware resulting in a data breach and damage to RFs reputation	2	4.1	5	41	70%	12.3
RF detects Entity non-public information has been exfiltrated resulting in a data breach	2	4	5	40	70%	12.0
A cyber security incident or system misconfiguration causes a NERC System(s) outage resulting in a major loss of employee productivity	4	2	2	16	30%	11.2
RF's infrastructure experiences an interruption resulting in moderate/total loss of communication resulting in the loss of employee productivity.	4	2	2	16	40%	9.6
RF non-public information is made available on the Internet and the public is aware resulting in a data breach and damage to RFs reputation	2	3	5	30	70%	9.0
RF detects that RF non-public information has been exfiltrated resulting in a data breach	2	3	3.9	23.4	70%	7.0



# SECURITY RISK REGISTER OVERHAUL

- Transition from “scattershot” approach to a risk generation system
- Align risk register controls with an industry standard
- Map the maturity of security controls to calculate effectiveness



# SECURITY RISK GENERATION SYSTEM

Actor/Agent	Type	Event	Asset Criticality	Asset/Resource	Outcome
Nature	Accident	Physical	Low	People	Damage
Affiliates	Intentional	Cyber	Medium	Company Brand/Reputation	Loss
Internal			High	Company Equipment	Outage
External			Critical	Facilities	
ERO				Cloud Technology	
Entity				IT Infrastructure	
Service Provider				Application	
				Information – Public	
				Information – Sensitive – Entity	
				Information – Sensitive – NERC	
				Information – Sensitive – RF	

## Security Risk Statements: Identification

- **255** potential Risk Statements
  - 6 Actor/Agents
  - 2 Types
  - 2 Events
- **15** Risk Statements with **Inherent Risk** of medium or higher

# SECURITY CONTROLS TAXONOMY

- Updated Existing Controls list to align with the NIST Cybersecurity Framework (CSF) 2.0
- Cross-referenced NIST CSF controls with filtered Risk Statements to assign applicability
- Developed “friendly names” for each NIST CSF control



# CONTROL EFFECTIVENESS

- Assessed maturity of RF controls in 2021, 2022, and 2023
- Used control effectiveness guidance to map maturity levels to percentages
- Reviewed each NIST CSF 2.0 Subcategory control and determined if it was applicable to reducing the risk of the top 15 Risk Statements

## Control maturity:

- 3, 4, or 5 = Existing Control
  - 1 or 2 = Developing Control
- Calculated an average Control Effectiveness and populated the Existing Controls and Developing Controls fields

# TOP RISK STATEMENTS

**MEDIUM  
(25)**

Sensitive Entity information for which RF is responsible is exfiltrated by an external malicious actor, resulting in a data breach and damage to RF's reputation.

**MEDIUM-LOW  
(15.8)**

A cyber security incident due to an external malicious actor causes the loss of RF's IT Infrastructure, resulting in loss of communication, loss of employee productivity, and negative financial impact.

**MEDIUM-LOW  
(15)**

Sensitive Entity information for which RF is responsible is exfiltrated intentionally by a malicious insider, resulting in a data breach and damage to RF's reputation.

Other Risk Statements have residual risk ratings of **Medium-Low**, between 12–15

# EMERGING THREATS



# CROWDSTRIKE OUTAGE

On July 19, CrowdStrike released a flawed configuration update for its Falcon security software, causing Windows computers to crash, disrupting internet services, and impacting hospitals, banks, and other critical infrastructure operations worldwide.

Impacts	Recovery
<ul style="list-style-type: none"><li>• Internet outage for an estimated 8.5 million Windows devices/computers</li><li>• Cancellation of 5,000+ commercial airline flights</li><li>• Financial losses of \$5.4 billion for Fortune 500 companies</li></ul>	<ul style="list-style-type: none"><li>• CrowdStrike's <a href="#">Remediation and Guidance Hub</a> provides steps to identify impacted hosts and restore cloud-based environments.</li><li>• Microsoft released a USB tool to aid outage recovery.</li></ul>
<h3>Lessons Learned</h3> <ul style="list-style-type: none"><li>• Be wary of consolidating critical technology among a small pool of service providers</li><li>• Protect critical infrastructure systems and business operations through digital resilience and redundancy</li><li>• Understand the platforms underpinning critical systems and avoid “single points of failure”</li><li>• Implement rigorous quality assurance testing before deploying code to production</li></ul>	

# RUSSIAN GPS JAMMING

## What Happened?

- During the Russian/Ukraine conflict, Russia **jammed GPS signals used by Ukraine's electric substations**, which rely on GPS for time synchronization.
- Global Positioning System (GPS) jamming involves **broadcasting a more powerful signal on the same frequency used for GPS**. The original GPS signal from a satellite is drowned out by the closer terrestrial broadcast.
- The Russian attack **prevented Ukraine's substations from reporting accurately to power dispatchers** and complicated efforts to balance loads, causing outages and failures.
- To combat GPS jamming, Ukraine **implemented equipment with enhanced mechanisms** that did not rely on GPS signals.

## Areas of Concern

- Russia's use of **GPS jamming is widespread** and has been reported throughout Europe.
- Security experts are concerned about **consequences of GPS interference in the event of Chinese escalation** around Taiwan. Chinese warships have been accused of interfering with the GPS systems of civilian airplanes throughout the Asia Pacific.
- Our concern regarding GPS interference is due in part to America's reliance on **outdated GPS technology (L1 signals) that could potentially be compromised by adversaries**. Deploying solutions that use signal technology in the L5 band could increase our resilience to GPS jamming.



# QUESTIONS & ANSWERS

Marcus Noel, Chief Security Officer

[Marcus.Noel@RFirst.org](mailto:Marcus.Noel@RFirst.org)

