NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Technology and Security Committee Open Meeting

August 14, 2024 | 8:30-9:45 a.m. Pacific

In-Person
Hyatt Regency Vancouver
655 Burrard St.
Vancouver, BC V6C 2R7, Canada

Conference Room: Regency A/B/C

Virtual Attendees
Webcast Link: Join Meeting
Webcast Password: Day108142024ATT (32910815 when dialing from a phone)
Audio Only: +1-415-655-0002 US Toll | +1-416-915-8942 Canada Toll | Access code: 2311 130 8233

Jane Allen - Chair
Larry Irving
Suzanne Keenan
Susan Kelly
Robin E. Manning
Jim Piro
Kenneth W. DeFontes Jr., *Ex Officio*

Introduction and Chair's Remarks

NERC Antitrust Compliance Guidelines

Agenda Items

1. **Minutes — Approve**
   a. May 8, 2024 Open Meeting*
2. **Technology and Security Committee Mandate* — Update**
3. **E-ISAC Operations*— Update**
4. **NERC Enterprise Analytics* — Update**
5. **Other Matters and Adjournment**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Technology and Security Committee
Open Meeting

May 8, 2024 | 9:45-10:45 a.m. Eastern
Hybrid Meeting

NERC DC Office
1401 H Street NW, Suite 410
Washington, D.C. 20005

Call to Order

Ms. Jane Allen, Committee Chair, called to order a duly noticed open meeting of the Technology and Security Committee (the Committee) of the Board of Trustees (Board) of the North American Electric Reliability Corporation (NERC or the Company) on May 8, 2024, at approximately 9:45 a.m. Eastern, and a quorum was declared present.

Present at the meeting were:

Committee Members
Jane Allen, Chair
Larry Irving
Suzanne Keenan
Susan Kelly
Robin E. Manning
Jim Piro
Kenneth W. DeFontes. Jr., *ex officio*

Board Members
Robert G. Clarke
Colleen Sidford
Kristine Schmidt
James B. Robb, President and Chief Executive Officer

NERC Staff
Tina Buzzard, Assistant Corporate Secretary
Manny Cancel, Senior Vice President and CEO of the E-ISAC
Mathew Duncan, Director Intelligence
Kelly Hanson, Senior Vice President and Chief Operating Officer
Stan Hoptroff, Vice President, Business Technology
Mark Lauby, Senior Vice President and Chief Engineer
Justin Lofquist, Director, Enterprise Application Architecture
Sonia Rocha, Senior Vice President, General Counsel, and Corporate Secretary
Camilo Serna, Senior Vice President, Strategy and External Engagement
Bluma Sussman, Director, Membership

NERC Antitrust Compliance Guidelines

Ms. Allen directed the participants' attention to the NERC Antitrust Compliance Guidelines included in the advance agenda package and indicated that all questions regarding antitrust compliance or related matters should be directed to Ms. Rocha.

Chair's Remarks

Ms. Allen welcomed participants to the meeting and reviewed the agenda. Ms. Allen also recognized Mr. Cancel and Mr. Hoptroff on their announcement that they plan to retire in early 2025. She thanked them for their efforts for the Committee, NERC, the ERO Enterprise and stakeholders.

Minutes

Upon motion duly made and seconded, the Committee approved the minutes of the February 14, 2024, open meeting as presented at the meeting.

E-ISAC Operations

Mr. Cancel and Mr. Duncan provided a summary of the cyber and physical security threat landscape facing NERC and the electricity industry. They discussed U.S. government policy matters related to incident disclosures, including SEC disclosure requirements and CISA's proposed critical incident reporting requirements. In addition, they summarized the findings of the recently issued 2023 Summary of Physical Security Incidents, shared insights from a recently completed pilot of aerial drone usage, and provided an update on 2024 election security preparations. Ms. Sussman updated the Committee on the progress of the E-ISAC Stakeholder Customer Experience (CX) and User Experience (UX) Project. She reported on the discovery phase of the project and next steps.

Following the presentations, the Committee discussed evidence of the use of drones against electricity infrastructure and capability to defend against such use; the relationship between CISA's new reporting requirements and NERC's reporting requirements; and the E-ISAC's insight into reporting by other sectors.

Business Technology Strategy

Mr. Hoptroff discussed NERC's Business Technology strategy. He discussed the objectives of the strategy and highlighted the critical investments under the strategy. Mr. Lofquist then also provided the roadmap for Align enhancements in 2024, noting that the focus areas are enhancing capabilities around audit and spot checks, periodic data submittals, self-certifications, attestations, compliance oversight plans, inherent risks assessments, and system confidence.

Following the presentations, the Committee expressed the desire to hear from users of Align on its impact on their interactions with NERC in relation to CMEP. The Committee also discussed the security of Align and the Security Evidence Locker, particularly as it relates to supply chain vulnerabilities.

Adjournment

There being no further business and upon motion duly made and seconded, the meeting was adjourned.

Submitted by,

Sônia Rocha
Corporate Secretary

Technology and Security Committee Mandate

Action
Update

Summary
As part of the annual review of all Board of Trustees Committee mandates, the NERC Legal Department has reviewed the current Technology and Security Committee mandate with the Committee Chair and members and is not recommending any revisions at this time.

E-ISAC Operations

Action
Update

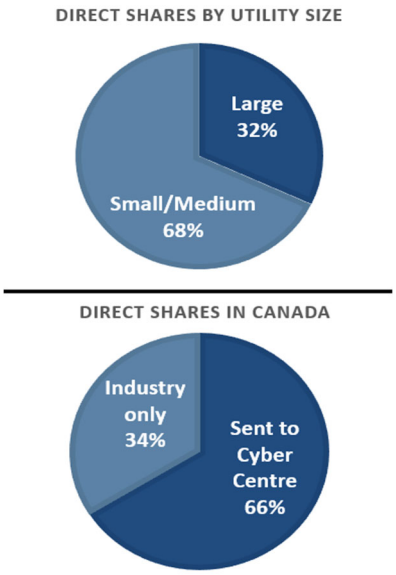
Summary
The threat landscape remains dynamic and complex for the electricity sector, involving actors ranging from nation-states to criminal organizations to extremists all looking to impact the reliable delivery of electricity across North America. The E-ISAC continues to deliver high quality information and analysis about these threats as well as risk mitigation advice to counter them. We will provide an overview of these activities at today's meeting. In addition, the E-ISAC will review its recent efforts to further improve the stakeholder experience and offer meaningful opportunities for our members and partners to learn, network, and engage. The E-ISAC looks forward to feedback from the Board of Trustees and the Member Representatives Committee and appreciates their continued support.

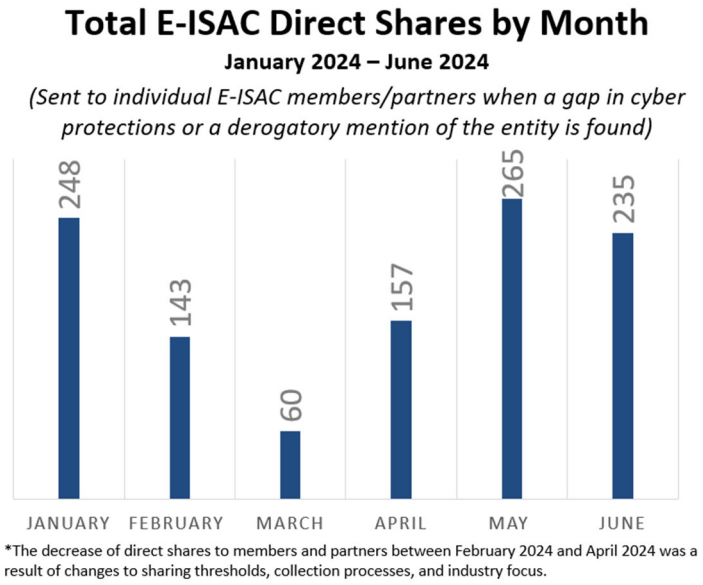
Security Operations and Intelligence Proactive Threat Identification
Adversaries constantly search gaps in our cyber and physical security programs to compromise the grid. This dynamic threat environment requires the E-ISAC to spot gaps proactively on behalf of industry using a variety of tools and sources before the adversaries do.

Direct Shares
Over the past three years, the E-ISAC formalized its monitoring program to provide direct shares of actionable information to members and partners. A "direct share" is sent only to a pre-identified member or partner's security team via email or phone call, as opposed to a "bulletin" which is posted to the E-ISAC portal and may be viewed by thousands of E-ISAC users. Direct shares result when the E-ISAC detects a gap or identifies a malicious reference to the member or partner. These gaps and references are typically found in open-source intelligence sources (e.g., internet searches or discussions on criminal forums). In addition to providing information on the detected gap or reference, the E-ISAC will send mitigation recommendations specific to the organization to support action to safeguard assets.

Through searches of available data sets (manual and automated) and the utilization of various tools, the E-ISAC leverages open-source intelligence (OSINT) and the dark web monitoring to provide proactive and actionable intelligence products in the form of direct shares. Currently each share is based on the criticality and specificity of the vulnerability found. Recipients of such shares have provided feedback that direct shares have significantly assisted in investigations, broadened awareness of the vulnerability and threat landscape, and enhanced overall security posture and resilience, adding to their layers of defense.

From January 1, 2024, through June 30, 2024, the E-ISAC sent 1,108 direct shares to stakeholders across the electricity industry and other critical infrastructure sectors (through each sector's ISAC) in the U.S. and Canada. Broken down further, 425 shares were sent to electricity industry asset owner or operator (AOO) member organizations and 682 shares were sent to interdependent E-ISAC partners (e.g. other critical infrastructure sectors, government partners). For context, electricity is just one of 16 critical infrastructure sectors, and while the E-ISAC's searches focused on electricity and gas AOO members, these searches often unearth potential threats or vulnerabilities to interdependent infrastructure, and we share our findings with their ISACs to increase collective defense and resilience. Furthermore, of the AOO member organization recipients, 68% are small and medium utilities, reflecting the rough breakdown in the type E-ISAC membership. While most of these shares were sent to U.S. organizations, Canadian partners and members received 59 direct shares with the Canadian Centre for Cyber Security receiving 66% of those shares.





For comparison, during the previous reporting period of July 1 to December 31, 2023, the E-ISAC sent 1,775 direct shares to stakeholders, with 619 shares being sent to AOO members and 1,156 to interdependent partners. Additionally, of the AOO member organization recipients, 73% were small and medium utilities, roughly consistent with the trend in 1H2024. The decrease in total shares in the first half of 2024 compared to the second half of 2023 period was the result of change in sharing thresholds, collection processes, and electricity and gas sector focus based off member feedback.

The trends over time are expected to evolve and be reflective of the threat environment and major vulnerability announcements. E-ISAC staff continue to evolve this service and are currently exploring ways to expand this offering through automation and process improvements with the goal of increasing the number of shares, including at lower levels of severity that could still be exploited by adversaries.

Threat Hunts

Since the middle of 2021, the E-ISAC has been conducting threat hunts in various sensor derived and other data sets. “Threat hunting” is a common and pro-active technique used by the U.S. and Canadian governments and cyber security firms to identify previously unknown vulnerabilities and compromises. Many electric utilities have their own internal threat hunting capabilities if they have the resources to do so. Threat hunts may be conducted if specific intelligence is available, or if analysts want to test a hypothesis about a type of malicious behavior.

Through its threat hunting activities, the E-ISAC offer research and analysis products to the electricity sector community by leveraging the various open and closed data sources correlated against data provided through the Cybersecurity Risk Information Sharing Program (CRISP). Hunts may take minutes or even weeks depending on scope, amount of data, or type of threat. However, guardrails, such as peer review and prioritization, are in place to ensure hunts do not continue indefinitely and always are documented to support continuous learning and analysis. Hunts may result in a direct share or a bulletin if sufficient and appropriately evaluated new information is found. These products draw on original and proactive research by E-ISAC analysts to assist industry in identifying anomalous and malicious events (supported by events observed within CRISP), and actionable mitigations for utilities of all sizes to better secure their networks.

The E-ISAC conducted 48 threat hunts in the first half of 2024; an increase compared to the same period in 2023 (30 total). The increase in 2024 resulted from increased hunt efficiency derived from automated sharing and improved analyst expertise. Some recent examples of these proactive threat hunts include:

- A hypothesis-driven hunt related to a known malware family called FlowCloud and the connection to an advanced persistent threat actor.
- An intelligence-driven hunt on a recently identified vulnerability in a widely used secure managed file transfer software.
- An intelligence-driven hunt related to known suspicious scanning for programmable logic controls of a heavily used vendor.

Many of the hunts result in reports with detailed technical analyses of the threats, tips for members to recreate the hunt in their own environment, and mitigation for all utilities to take to secure their infrastructure. While no compromises were detected, the threat hunts identified areas of vulnerability that utilities were better able to secure.

Physical Security Capabilities and Programs

Given the observed rise in serious grid impacting physical incidents, the E-ISAC continues to promote physical security best practices and risk mitigation approaches. The most impactful of these offerings include a variety of in person workshops designed to teach skills and convene stakeholders across the continent to better understand physical security risks.

Vulnerability of Integrated Security Analysis (VISA) Workshops

The E-ISAC began conducting VISA workshops in 2018, in response to industry's growing demand for a cost-effective, risk management tool. Following a design basis threat (DBT) methodology developed by Pacific Northwest National Lab (PNNL), VISA workshops provide utilities with a unique opportunity to sit down with their internal and external partners to determine the effectiveness of their systems. VISA workshops enable utilities to identify critical mitigation measures needed to protect their assets from a growing fleet of adversaries looking to attack their infrastructure. At the end of the workshop, utilities are provided information explaining the security risk need for upgrades which enable their leadership to make risk informed and cost-effective decisions.

To date, the E-ISAC has conducted over 20 workshops for various types of utilities across the U.S and Canada. In 2024, the E-ISAC has already held three out of the seven planned workshops. The E-ISAC will look to evolve this program in the coming years as cyber and physical security streams begin to converge into hybrid threats and demand from industry grows.

Physical Security Regional Workshops

At the strategic level, in response to the evolving physical threat landscape impacting the electric industry, the E-ISAC continues to conduct its series of Regional Physical Security Workshops in partnership with the Electricity Subsector Coordinating Council (ESCC). The first workshop took place in the fall of 2023 in Charlotte, NC, in partnership with EEI, APPA, NRECA, EPRI, SERC, and Duke Energy. The most recent workshop was held in May 2024 at Puget Sound Energy's headquarters in Bellevue, WA and included more than 100 participants from different utilities across the U.S. and Canada, as well as government partners and law enforcement agencies.

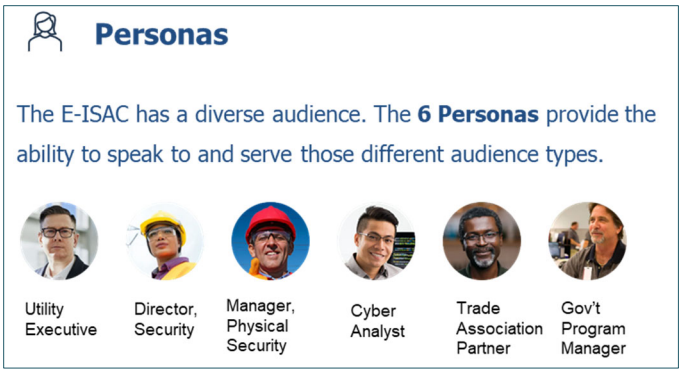
The workshops provide a unique forum to establish new connections and exchange critical information on the most concerning physical security threats to the North American grid. The workshops also help utilities share information on mitigation strategies and best practices to protect their assets from the risks posed by the complex and dynamic physical security landscape. A third workshop will take place in Chicago, Illinois in September 2024.

Stakeholder Experience/User Experience

The objective of our stakeholder experience effort is to increase the value of the E-ISAC and support the electricity industry's collective defense. The work we are doing around stakeholder experience touches every facet of the E-ISAC's service offerings to its 1800 member and partner organizations and will be critical in driving our strategy for years to come.

The E-ISAC continues to engage with Main Digital, to identify areas of improvement for our stakeholders. Leveraging direct feedback from E-ISAC members and partners, Main Digital is analyzing the customer (stakeholder) experience, defining stakeholder personas, identifying gaps in our engagement, and assessing the Portal user experience. The resulting recommendations will help the E-ISAC continue to increase its reach and minimize friction for its stakeholders.

Personas and Journey Maps



Earlier this year, Main Digital surveyed and interviewed representative samples of E-ISAC membership and staff. The analysis informed development of proposed stakeholder personas and future-state stakeholder journeys. Six user personas (detailed characters representing various types of users or stakeholders) were developed which provide the E-ISAC with the ability to better speak to and serve those unique audience types. These personas include attributes such as organization type and size, job level, digital preferences, etc.

The Main Digital team completed a friction map to assess current gaps and opportunities for stakeholder engagement across personas, which provides a visual depiction of a stakeholder's journey with a focus on identifying customer challenges that lead to frustration, or "friction" in their experience. For example, if a user cannot easily access security threat information on the Portal, they may be less inclined to log in, which can create friction in the stakeholder experience.

Using data from the personas and friction maps, Main Digital developed future-state journey maps associated with each persona, which visualize the end-to-end stakeholder experience to help shape the stakeholder lifecycles for E-ISAC members and partners and support the development of strategic engagement initiatives that are timely and impactful.

Service Blueprint

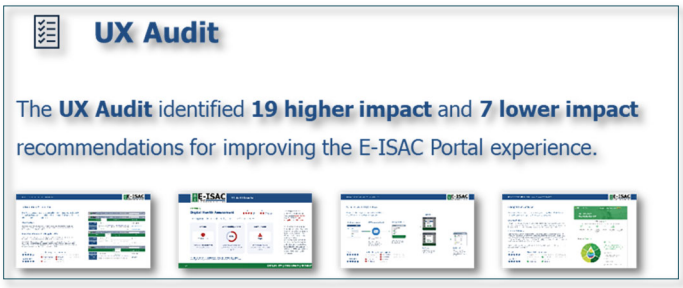
Phase two of this project included development of a service blueprint, a diagram which visualizes the processes involved in delivering services to E-ISAC membership, including both frontstage activities (visible to stakeholders) as well as backstage activities (behind-the-scenes) activities. The service blueprints will help the E-ISAC better understand how services are delivered, and identify areas of strength, areas for improvement or new processes that should be established to provide stakeholders with a more mature stakeholder experience and inform development of the stakeholder engagement plan.

Proposed Stakeholder Engagement and Measurement Plan

Main Digital has identified current methods of measurement across the E-ISAC (surveys, data analytics, qualitative feedback processes, engagement dashboards) and mapped these metrics to the persona journey stages. The combined plan proposes Key Performance Indicators (KPIs),

Objective and Key Results (OKRs) and action steps to drive future stakeholder engagement and measure progress. These tools, along with stakeholder engagement dashboards the E-ISAC is developing, will help continuously refine our stakeholder experiences to best inspire members and partners to protect their critical infrastructure.

Portal User Experience Audit



Main Digital also recently completed a user experience audit of the E-ISAC Portal and summarized their findings and recommendations. They identified 19 "high impact" and an additional 7 "lower impact" opportunities to address usability issues, enhance content delivery, improve design effectiveness and strengthen brand conformance, thus creating a more digestible and actionable digital experience for our stakeholders. Examples of high impact recommendations include brand optimization, Portal design and accessibility redesign, typography and iconography and notification preferences refactoring. Examples of lower impact opportunities include updated button and link styling, improving naming clarity/consistency and improving instruction copy. These recommendations will inform the evolution of our E-ISAC engagement strategy, including future Portal enhancements.

Next Steps

Looking ahead, enhancing the stakeholder experience will inform the E-SIAC strategy for the coming years. The information that we learn through this effort will drive engagement activities across the entire E-ISAC. In Q3 2024, the Stakeholder Engagement Team will leverage the resources offered as part of this initial engagement to develop a strategic stakeholder engagement plan. This plan will drive future engagement initiatives, inform on-going, monthly Portal enhancements and drive resource needs and allocations to provide E-ISAC stakeholders with the level of quality information, analysis, and opportunities to engage in support of our collective defense.

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Operations Update

Manny Cancel, Senior Vice President and E-ISAC CEO
Bluma Sussman, Vice President, Stakeholder Engagement
Matt Duncan, Vice President, Security Operations and Intelligence
August 14, 2024

TLP:CLEAR

RELIABILITY | RESILIENCE | SECURITY



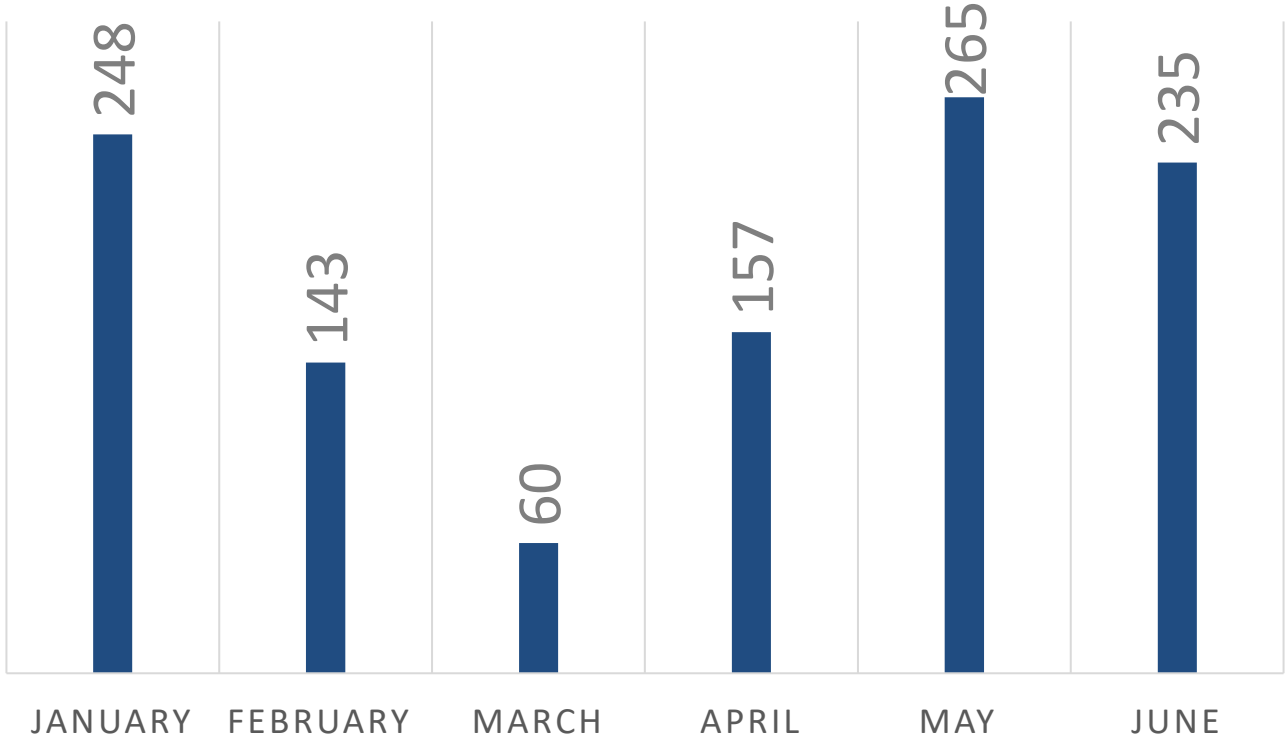

E-ISAC Security Operations and Intelligence Update

Direct Shares

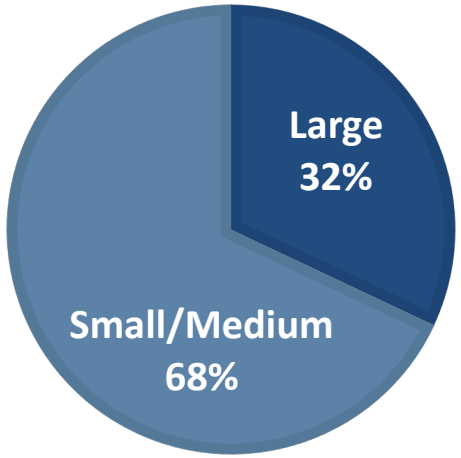
Total E-ISAC Direct Shares by Month

January 2024 – June 2024

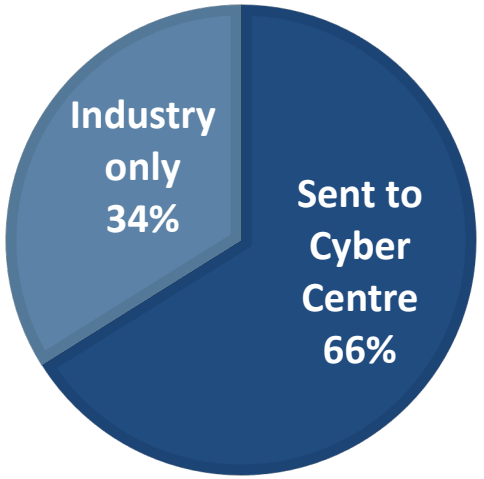
(Sent to individual E-ISAC members/partners when a gap in cyber protections or a derogatory mention of the entity is found)



DIRECT SHARES BY UTILITY SIZE



DIRECT SHARES IN CANADA



Recent E-ISAC Threat Hunts

Hypothesis driven hunt to identify malware associated with nation-state actor(s)

Intelligence driven hunt to identify recent vulnerabilities

Intelligence driven hunt to identify scanning of programmable logic controllers

Vulnerability of Integrated Security Analysis (VISA) Workshops

20 workshops conducted since 2018 for U.S. and Canadian utilities

367 individuals have taken part in VISA

81 organizations attended (utilities, gov)

7 workshops scheduled for 2024 (3 completed)

Regional Physical Security Workshops

E-ISAC
ESCC
Electricity Subsector Coordinating Council
DUKE ENERGY
RELIABILITY FIRST
EPRI
EEI
Edison Electric INSTITUTE
comed
AN EXELON COMPANY
PSE
PUGET SOUND ENERGY
SERC
Reliability Corporation
NRECA
America's Electric Cooperatives
AMERICAN PUBLIC POWER ASSOCIATION
WECC

E-ISAC Stakeholder Experience

Stakeholder Experience: Discovery to Development

16 E-ISAC Staff Interviewed

07 E-ISAC Members Interviewed

03 E-ISAC Partners Interviewed

60 Question Survey about Behaviors

70 Member and Partner Responses

06 Core Personas Created

Personas: A Targeted Approach to Stakeholder Engagement

Personas

The E-ISAC has a diverse audience. The **6 Personas** provide the ability to speak to and serve those different audience types.

Utility Executive

Director, Security

Manager, Physical Security

Cyber Analyst

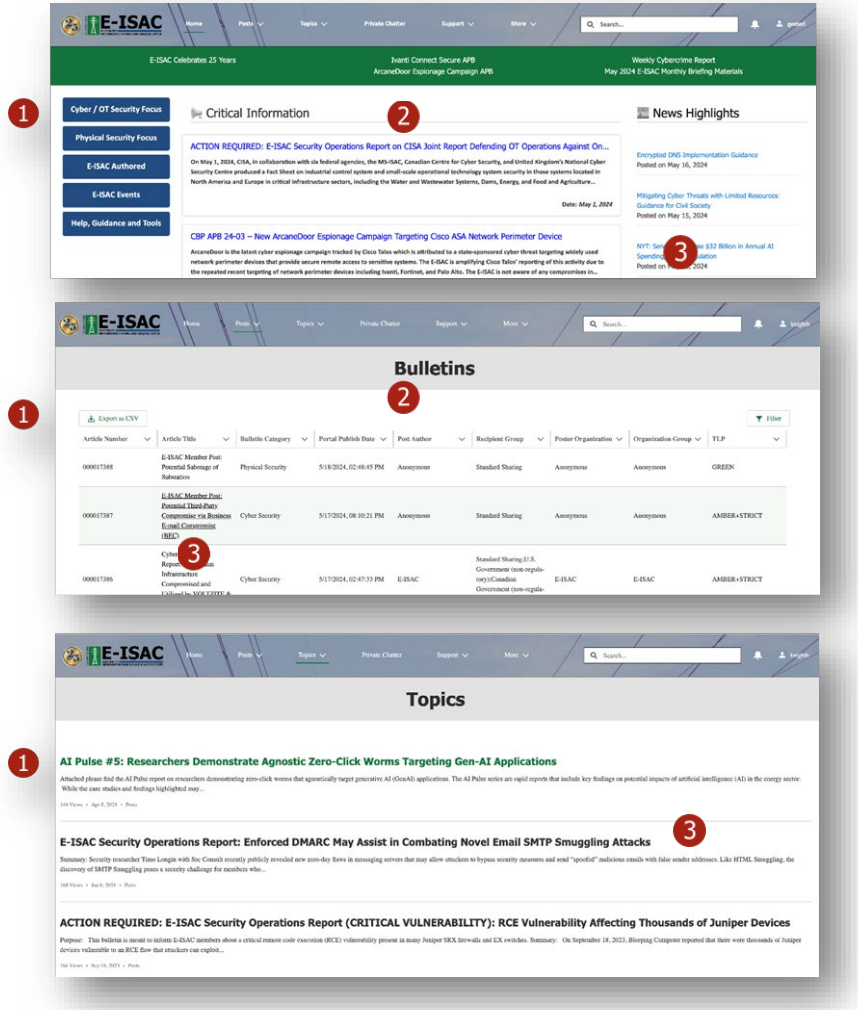
Trade Association Partner

Gov't Program Manager

Portal User Experience Audit

Core facets of user experience

1. Usability
2. Design Effectiveness
3. Brand Conformance
4. Content Delivery
5. Accessibility



UX Audit Recommendations

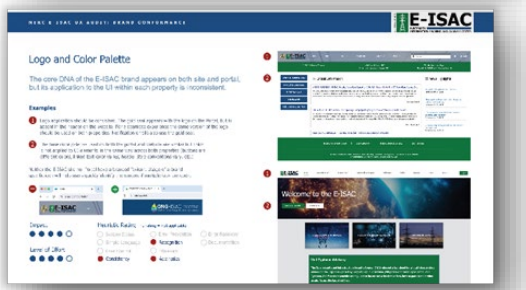
19 Higher Impact

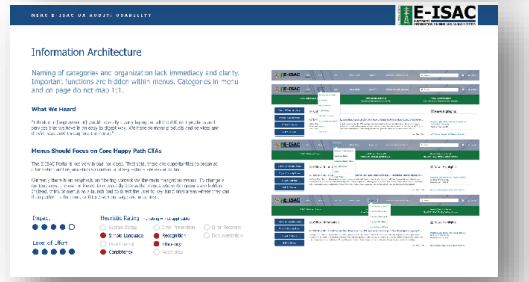
- Brand optimization & new design system
- Portal redesign
- Accessibility redesign
- Information architecture improvements
- Notification preferences refactoring
- Typography and Iconography
- Delivery Frequency

+ 12 more

07 Lower Impact

- Update button styling
- Update text link styling
- Improve naming clarity / consistency
- Improve instruction copy
- Strengthen calls-to-action
- Improve page elements & layout
- Refactor content access & filtering





Measurement: Success Metrics

How Do We Define Success?

Fulfill E-ISAC's mission

Reduce cyber and physical security risk to the electric industry across North America by providing unique insights, leadership, and collaboration

Information that is timely, relevant, and actionable

Solve member problems

Email notification-to-Portal friction

Too much information and noise

Fulfill member needs

Understand threats and take action when necessary

Build relationships

Stay aware and informed

Maximize member engagement

Ease digital interaction

Reduce friction and barriers to engagement

Increase event participation

Questions and Answers

Agenda Item 4
Technology and Security Committee
Open Meeting
August 14, 2024

Enterprise Analytics

Action
Update

Summary
Using data to make informed business decisions is a priority in NERC's 2026-2028 three-year planning efforts, and NERC will be advancing its analytics capability to support the areas of Energy Assessments, Bulk Power System Awareness, Power Systems Analysis and Transfer capability.

In this discussion, management will highlight some successes the Business Technology function has had in facilitating Enterprise Analytics across the ERO Enterprise and how we're contemplating the future of opportunities in the analytics space. This includes the challenges we face and how NERC is tackling them. This is a continuing journey of learning, building on earlier successes and defining a vision for the future.

What is Enterprise Analytics?
Enterprise Analytics is about transforming data into a strategic asset. A collection of tools, techniques and policies that are brought together to build what's needed to achieve this goal. This includes collecting and moving the data to the right locations, storing it security, and applying tools to analyze it. For NERC, critically it also includes providing data to stakeholders in a secure manner to support their analytical needs.

The starting point to any effort within the Enterprise Analytics circle is the data, beginning with the question "Which data"? To answer this, NERC has a very tight scope of which data we consider for inclusion into the analytics space. For example, we don't bring in entity compliance information, and certainly nothing from the Secure Evidence Locker, as this data is highly sensitive and therefore is isolated from other business data. Instead, we focus on facility performance and registration information, as this data provides valuable insights into grid reliability.

As we open the lens of analytics, security and availability wrap around the data we possess. Fundamentally, we're concerned about two things: 1) preventing bad actors from coming in and getting the data, and 2) ensuring only the right people get the data that's shared. Combating these threats requires sophistication and diligence, with everyone understanding and fulfilling their role in protecting the data, from system administrators to end users. Only after we can confidently secure the data can we provide business users with the ability to draw insights

through analytics; enabling them to make more informed business decisions based on those insights.

This enterprise analytics "stack" requires ancillary pieces to be successful. Data protections (including data loss prevention), optimized infrastructure, training and business knowledge are all necessary to build a successful analytical capability.

Business Insights – Early Successes

The NERC analytics team is following a Crawl, Walk, Run Methodology, starting small and building on our early successes. This way we can learn, not just from our mistakes, but also about the capabilities of the technology and the best way to use it. Some highlights from our early successes are below. They include solutions to provide data to other stakeholders to further enhance their analytical capabilities, as well as building NERC's own analytical environment.

1. **Provisioning Data to FERC:** In 2016, FERC Order No. 824 directed NERC to share with FERC US-only data from (1) the Transmission Availability Data System, (2) the Generating Availability Data System, and (3) the Protection Systems Misoperations Database. The implementation resulted in a single, secure connection between NERC and FERC, by which FERC can directly access the most current set of transmission / generation performance and misoperation data for the United States. With this access, FERC has better visibility into industry operations and is utilizing the data to generate analytical studies, including a recent analysis of extreme weather effects on transmission outages.

2. **Providing Data to Regions:** One of the most compelling and value-added success stories has been NERC becoming a data provider to Regional Entities. Regional Entities can now securely and reliably access data collected by NERC and combine it with data they collect to perform regionally directed analysis. The solution has the flexibility to support varying levels of Regional Entity analytical maturity, while consolidating access of this data to a single endpoint. In addition, because all Regional Entities are working with the same set of data, we avoid many of the inconsistent conclusions that occur when everyone has their own copy of the data. Most importantly, Regional Entities access this data in a completely automated and secure fashion, avoiding the need for users to download the data by exporting reports from applications.

   To date, the following data sets are included: registration (including joint registration constructs), generation (including traditional and wind), transmission, and protection systems operations information.

3. **Providing Analytics to NERC:** There have been several successes related to providing data services to the NERC organization, including the creation of a NERC Analytics Hub. This user self-service solution provides a single place where users can bring in data from different sources, then model that data to generate reports, visualizations, perform complex analytics and securely distribute work products.

   Another success is the set of orchestrated data integrations between systems, so applications are all using data from a single source – for example we don't have multiple entity registration lists, one in each application.

The consistent theme with these successes has been the continual advancements in protecting the data through technology and process. By pulling the data into highly secure, IT-managed solutions and implementing industry best practices, we're able to leverage sophisticated solutions to keep the data secure.

Increasing Analytical Capabilities

Looking at how the NERC Analytics Hub is being adopted, NERC finds our business units following similar journeys. Typically, it starts with users identifying the pain of having to work within Excel to find, combine and work with data, just to satisfy simple operational reporting needs. As they start using the analytics hub to solve that issue, their comfort with technology grows and they start exploring more and more capabilities. For example, we start seeing more complex visualizations, more users loading their own data into the environment, and more interesting insights being drawn. There is no real end to the journey, as there will always be more data to be brought in and insights discovered. Using technology to its fullest, bringing together multiple different types of data, incorporating analytics into part of core business operations, and gleaning new, unexpected insights are all indicators of a highly effective analytics function. We recognize that success in large part is dependent on the support these business units receive from the IT function – responsiveness, education and collaboration.

Business Insights – What's Next?

The NERC team will continue to execute existing strategic efforts while continually looking for new opportunities to apply analytics to support the ERO mission. This includes:

1. **Establishing an ERO Enterprise Analytics Hub for Regional Entities**: Building on the success of the NERC Analytics Hub, the team is currently establishing the scope of the ERO Enterprise Analytics Hub in conjunction with the Analytics Collaboration and Excellence (ACE) group, This working group is comprised of Regional and NERC analytics professionals charged with creating a vision for a single, collaborative analytics environment for the ERO Enterprise. The ERO Enterprise Analytics Hub will allow regions and NERC to:

    a. Collaborate across the ERO Enterprise to develop analytical models and share that work with others across the enterprise.

    b. Use the analytical work from others as a starting-off point, tailoring it to their specific needs.

    This environment will offer teams a starting point for their own analytical needs, significantly reduce duplicative efforts and support the ongoing development of analytics capabilities across the enterprise. Most critically, as all the data will remain in the hub at rest, this environment will eliminate the need to have data reside in multiple locations within the ERO Enterprise, thereby decreasing the attack surface for bad actors.

2. **Tailoring Stakeholder Engagement for NERC**: Enterprise analytics also plays a significant role in NERCs stakeholder engagement strategic initiatives. We are building programs to gather direct engagement data from our digital platforms to tailor our stakeholders' experience. For example, generating visit analytics from NERC.com will allow us to better understand individual stakeholder behaviors and preferences and then tailor their experience, interactions, and communications to their specific needs.

3. **Enhancing Industry Benchmarking for Load Serving Entities**: The most compelling program on the horizon is providing modern benchmarking capabilities for industry. Our current industry benchmarking offering is static with limited analytical functionality, restricted to the performance of traditional generation. We will broaden our industry benchmarking offering to include transmission, protection systems, and other performance-based metrics on demand, using current data with modern analytical tools.

Challenges Ahead

As we continue to expand our analytical capabilities for the entire enterprise, we will face many challenges. First and foremost, the ERO Enterprise is a complex environment, and this program is a complex undertaking. Additionally, every organization in the enterprise has their own set of priorities. We need to operate in a way that addresses individual priorities, while also placing importance on those shared priorities that benefit everyone.

Finally, and most importantly, the challenge of protecting the data is ever-present. As bad actors get more sophisticated with their approaches, we need to ensure both technical and procedural controls are properly implemented and maintained.

How Do We Get There?

Five years ago, the Analytical Collaboration and Excellence (ACE) Group was formed. Consisting of representation from NERC and each Regional Entity, its charter is to develop, support, and continually improve qualitative and quantitative analytical processes for the enterprise, while encouraging the use and sharing of common tools and techniques among NERC and the Regional Entities.

This group works closely with their IT counterparts in the ERO Enterprise IT Knowledge Sharing group to drive forward a shared vision for ERO Enterprise analytics. The most valuable part of the group is shared knowledge. It enables members to think more broadly than they otherwise would. We find that especially valuable when building line-of-business applications to collect data. The group is thinking about how the collected data relates to existing data sets, from an enterprise analytics perspective.

Additionally, the ACE looks ahead to challenges facing the program, many of which require the type of collaboration the team is already performing. As we move toward building the ERO Enterprise Analytics Hub, heavy attention is being paid to how we protect the data in this new environment. Outside the traditional technical solutions (e.g. firewalls or spam blockers), the group recognizes that procedural controls are very effective in ensuring work products are distributed only to intended parties and will be contributing to the creation of those procedures as part of their charge.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Enterprise Analytics

State of Affairs

Justin Lofquist, Director of Enterprise Applications Architecture
Technology and Security Committee Open Meeting
August 14, 2024

RELIABILITY | RESILIENCE | SECURITY




What is Enterprise Analytics?

- ✓ Data Protection
- ✓ Infrastructure Optimization
- ✓ Training and Business Knowledge

Building on early successes to scale new capabilities to stakeholders

Providing Data to FERC

"Through Order No 824, NERC is contributing to FERC's overall mission to have better visibility to industry operations."

-Donna Pratt
NERC Performance Analysis Manager

Providing Data to Regions

"We are able to build on these risk-mitigating and resilient analytical solutions by combining with external data sources, such as NOAA and EIA data to provide additional insights into industry performance."

-Angie Colacarro
ReliabilityFirst Manager of Analytic Services

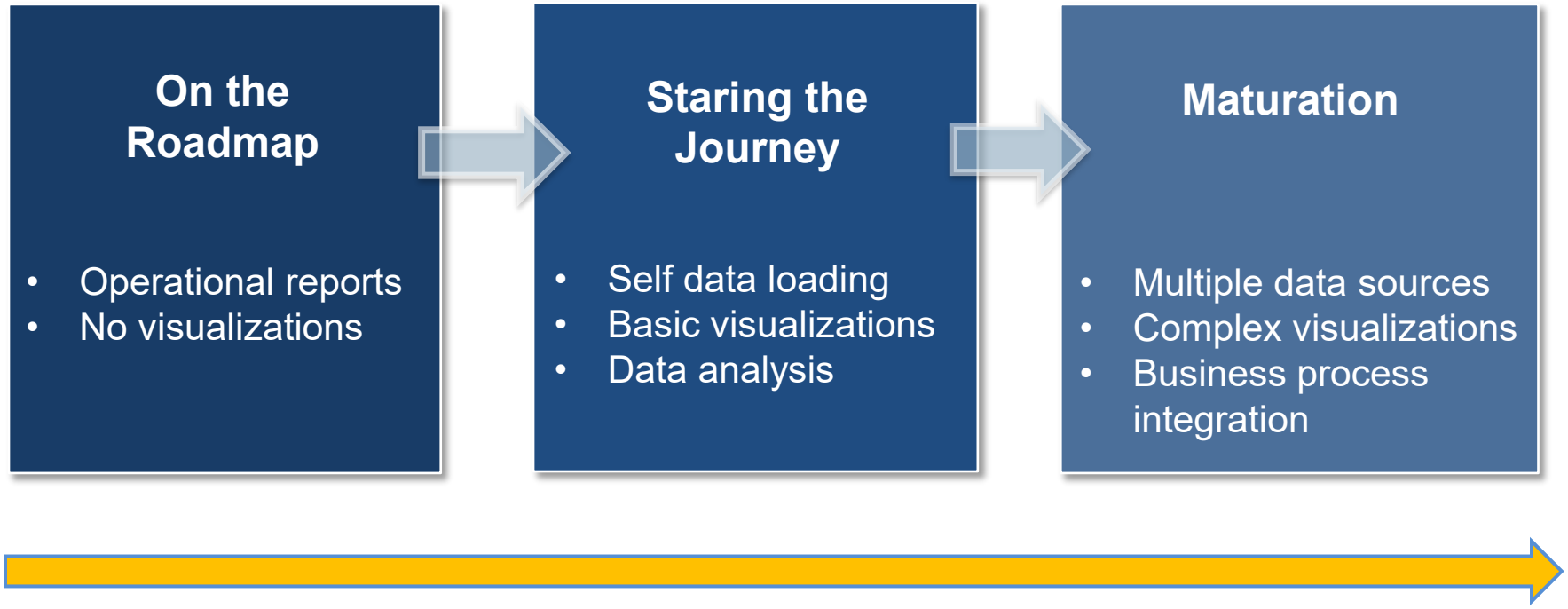
Provisioning Analytics Hub to NERC

"[The solution] is assisting the EA program in building analytical responsiveness, flexibility, and adaptably in our world of system performance monitoring and forensics."

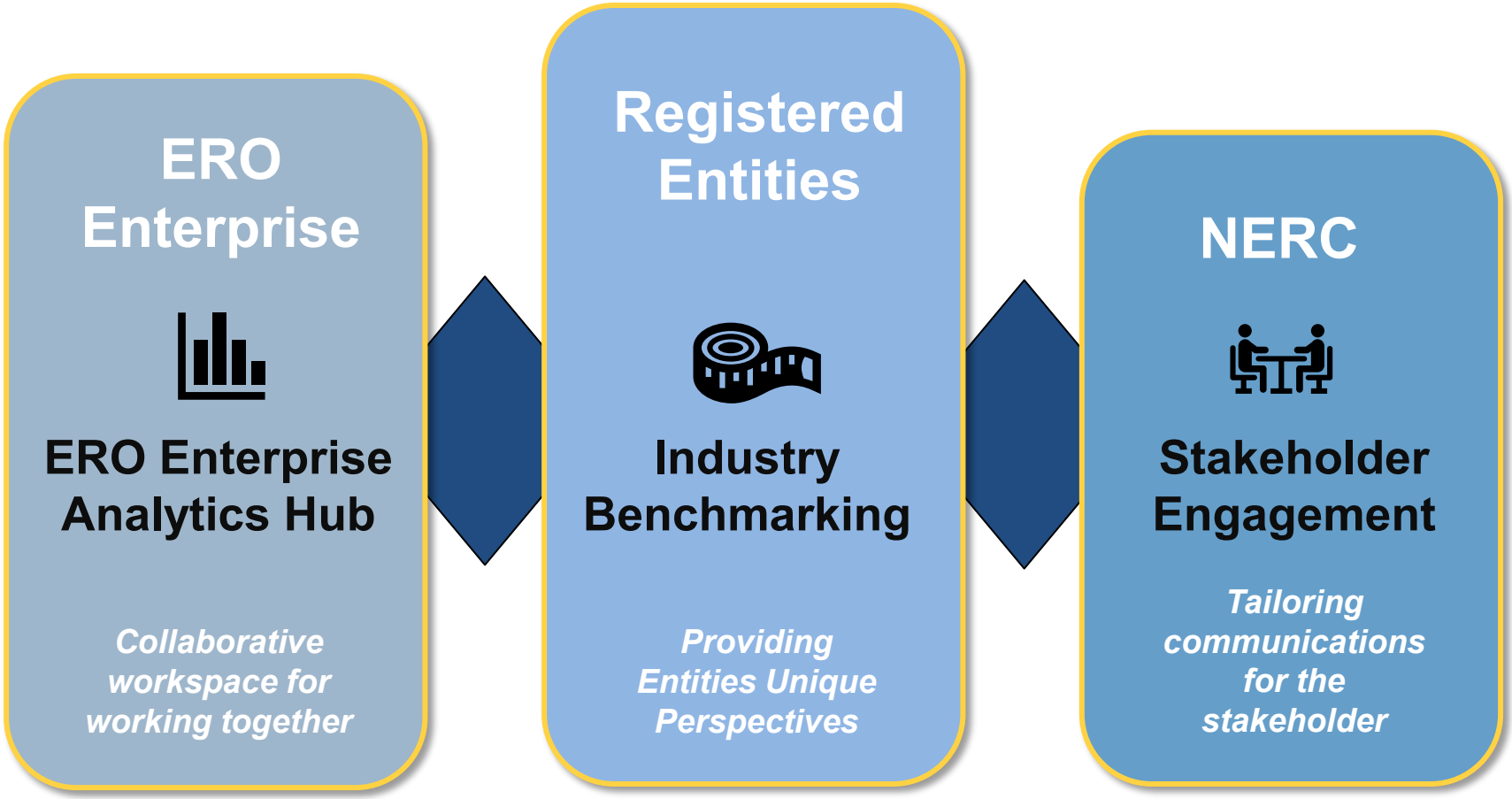
-Matt Lewis
NERC Manager – Events Analysis

Increasing Analytical Capabilities

Working jointly with business users to advance their self-service analytical capabilities



Upcoming initiatives will deliver value to a broad set of stakeholders



Challenges Ahead

Anticipating challenges so they don't become roadblocks

- Competing priorities
- Regional differences in analytical maturity
- ERO Enterprise complexity
- Data protection

How do we get there?

Analytics Collaboration and Excellence (ACE) Group

Data Analytics professionals from across the ERO Enterprise collaborating to create a shared vision

- ☑ Enterprise perspective of the data
- ☑ Sharing knowledge and insights
- ☑ Establishing priorities
- ☑ Governance and data management

Questions and Answers