NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

E-ISAC Strategic Plan

Manny Cancel
Technology and Security Committee Open Meeting
May 13, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

- COVID-19
- Landscape Assessment
- Progress to Date
- E-ISAC Strategic Plan
- Resource Focus
- Near-Term Focus
- Long-Term Focus
- Keys to Success

COVID-19

E-ISAC has been actively tracking COVID-19 since February 2020

- Business continuity plan activated and entire E-ISAC working remotely
  - Watch Operations fully staffed
  - CRISP online and functioning
- Portal postings and Level 2 NERC Alert issued
- Engaging and supporting Government partners
- Participating in ESCC Tactical Tiger Teams
- Maintaining contact with Tri-Sector entities

ISAC Landscape Assessment

- Quantitative assessment of critical infrastructure ISACs conducted
- Key Findings:
  - The E-ISAC is a well-established organization, with comparable resources and offerings to the top tier of the assessment group (the Financial Sector and Multi-State ISACs)
  - The E-ISAC is financially sound, with appropriate costs relative to staffing and offered products and services
  - Opportunities for improvement include project prioritization, demonstrating the value of and increasing member information sharing, and increasing membership of public power

Progress to Date

Organizational Changes:

- Leadership and other key positions strengthened
- Security operations reorganized and 24x7 Watch established in shakedown mode
- Performance Management Group established and formal project management principles adopted

Operational and Other Improvements:

- Increased information sharing and Critical Broadcast Program
- Cybersecurity Risk Information Sharing Program (CRISP) governance improved; CRISP expansion continues
- Customer relationship management system implemented and membership expanded
- Memorandums of Understanding (MOUs) executed with Independent Electricity System Operator, Department of Energy, and other ISACs
- Performance metrics put in place (See Appendix)

Operations Update

24x7 Staffing in Place (Remote)

- Fully Operational in Q3 2020 or sooner
- Cyber and Physical security watch shifts in place staffed by employees and contractors
- Two week schedules in place and adjusted as needed
- Key Functions
  - Threat Analysis
  - Portal Postings and Administration
  - Process Improvement
  - Training, Drills, and Procedure Development

Threat Landscape

Cyber

- **COVID-19 Threats**
  - HHS Denial of Service (DoS) attack
  - Remote access and collaboration facilities
  - Disinformation, spearphishing, and credential harvesting
- **U.S. / Iran Tensions**
  - Activity is reduced but Iranian threat actors remain active
- **Other Threats**
  - ICS Supply Chain
  - Collaboration sites (DropBox, Google Drive, O365)
  - Phishing and credential harvesting
  - Ransomware and destructive wiper malware

Threat Landscape

Physical

- **Theft**
  - Represents 47% of the total incidents shared with the E-ISAC
  - Copper theft accounts for 50% of thefts
  - Most incidents (42%) are in substations
- **Intrusions**
  - Trespassing and intrusion account for 21% of incidents
  - Most incidents (51%) are in substations
- **Surveillance**
  - Suspicious photography, reconnaissance and drones account for 11% of incidents shared

CRISP Update

- New governance framework in place
- Operational Technology (OT) Pilot in progress
  - RFP sent to vendors, final responses due May 15
- System Log Pilot
  - Assimilate logs into CRISP and enhance ability to check for threats
  - Target for production Q1 2021
  - Will be incorporated into 2021 CRISP budget
- Medium and Small utility cooperative initiative
  - In discussions with DOE, NRECA, and APPA

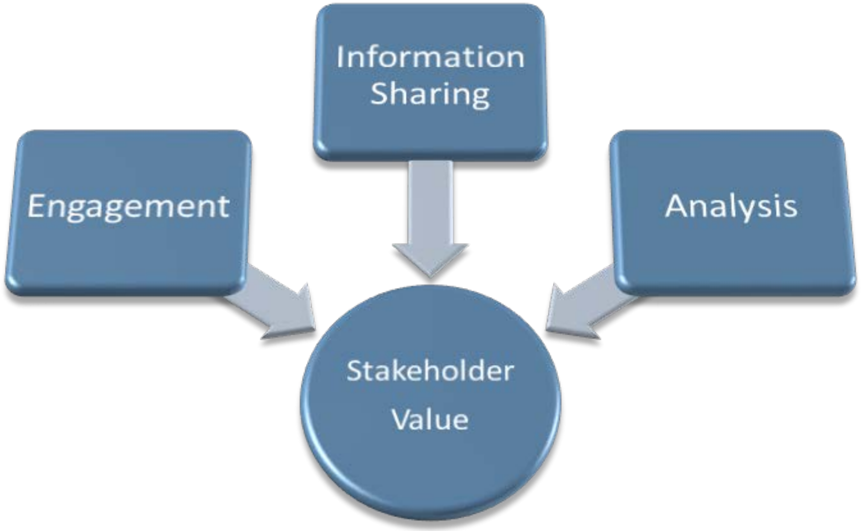
Engagement Update

- Events
  - Schedule under review and upcoming events switched to web conferences
  - March IEP and GridSecCon canceled due to coronavirus/travel restrictions
- Member Feedback Strategy
  - Formalize process to collect, manage, and respond to member feedback in Q2 2020
  - Create and implement member feedback survey (bi-annual)
- Designated Approving Official Rollout
  - Enhance member onboarding experience
  - Streamline internal processes for onboarding/vetting
  - Members knowledge and control of Portal access by their organization
  - Improved ability to communicate with member organizations

E-ISAC Strategic Plan

Focus Areas:

- Timely and actionable information
- Analysis regarding security threats and mitigation strategies
- Improved collaboration with industry, U.S. and Canadian government partners, and other stakeholders
- Continuous improvement and alignment across our three strategic pillars



Resource Focus

- Maximize resource utilization
- No significant personnel increases
- Evaluate and prioritize strategic relationships
- Effectively increasing information sharing
- Assess ability to add significant value to members through internal data enrichment strategies and investments
- Define role regarding operational technology risk identification, assessment, and information sharing

Near-Term Focus (2020-2021)

Organizational Initiatives

- Continue to foster an inclusive work environment, optimize organizational structure
- Refine succession plan for key roles
- Establish 24x7 Security Operations
- Consider use of service providers to supplement operations, technology initiatives, and key conferences (GridSecCon and GridEx)

Operational and Other Improvements

- Demonstrate the value of increased information sharing
- Support U.S. and Canadian government initiatives
- Complete CRISP +30 and Operational Technology (OT) pilot and evaluate other sensors
- Use feedback to improve member services and increase membership in underrepresented areas
- Operationalize and extract value from recently executed MOUs

Prioritizing Strategic Partnerships

- High Priority Partnership
  - Formalize and expand engagement and collaboration
  - Explore data sharing opportunities

U.S. DEPARTMENT OF ENERGY

Homeland Security

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

ieso

DNG-ISAC

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

- Other Partnerships and Relationships
  - Nurture with reduced E-ISAC resource commitment

ONG-ISAC Information Sharing & Analysis Center
Fueling the Exchange of Cyber Intelligence

WATER ISAC

EE-ISAC

JE-ISAC

FSARC

MITRE

Long-Term Focus (3-5 years)

- Adopt a broader focus on OT risks
- Develop enhanced threat and intelligence analytics
- Extend services to the downstream natural gas sector
- Continue to evaluate partnership opportunities with:
  - Commercial sector
  - Other ISACs
  - Government sponsored research and development organizations

The E-ISAC will engage stakeholders and government partners to carefully evaluate the benefits and potential challenges of each of these initiatives

Keys to Success

- Allocating resources more effectively
- Demonstrating the value of information sharing
- Improving decision-making and governance
- Enhancing project prioritization and management
- Increasing engagement and collaboration

Performance Metrics

Metrics - Engagement

Total Portal Users:

8,153

7,707 Members

446 Partners

Total Organizations:

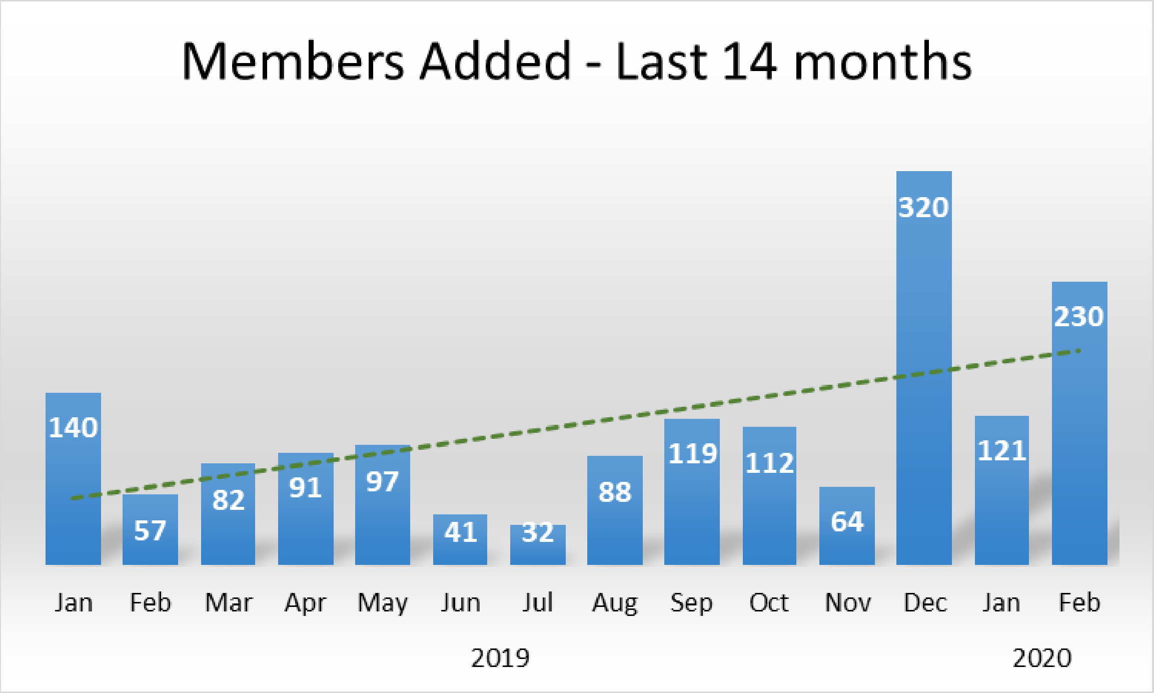
1,275

1,168 Members

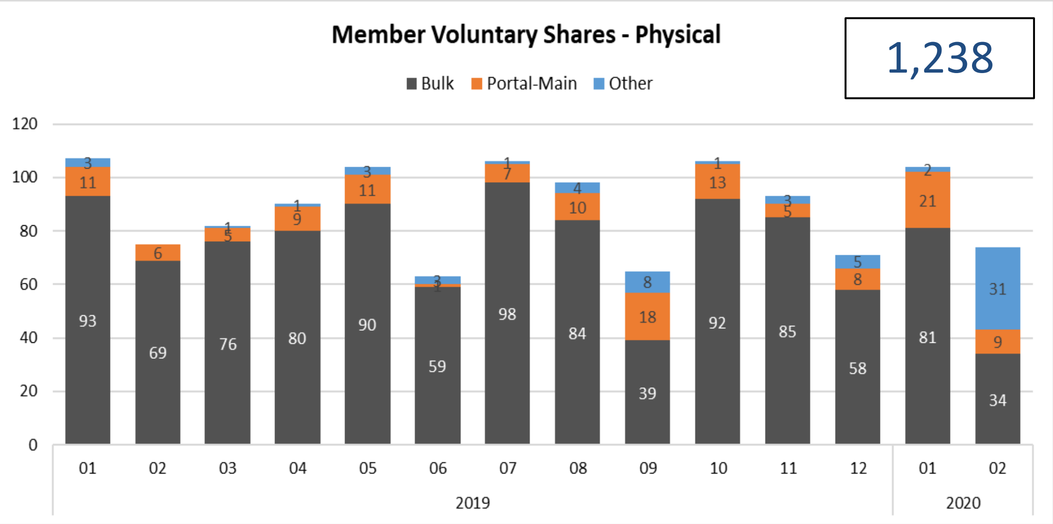
107 Partners

Coverage:

35% of utility orgs. servicing ≈ 75% of end customers collectively



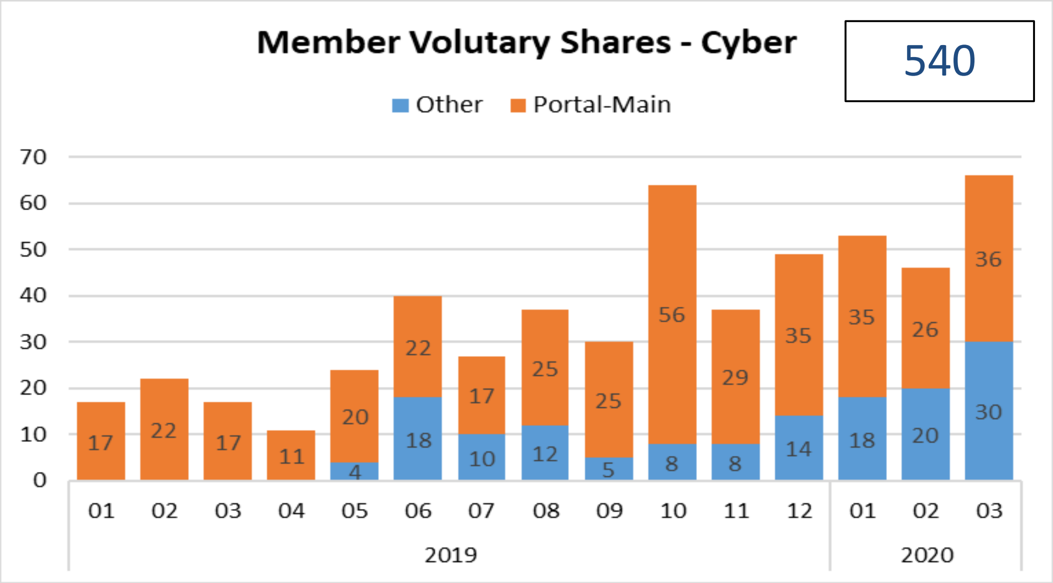
Metrics - Information Sharing



1,238

Physical

- 59 unique member organizations had at least one physical share (Jan’19-Feb’20)
- 81% of all shares came from two members
- Most sharing came outside of the Portal (via bulk)



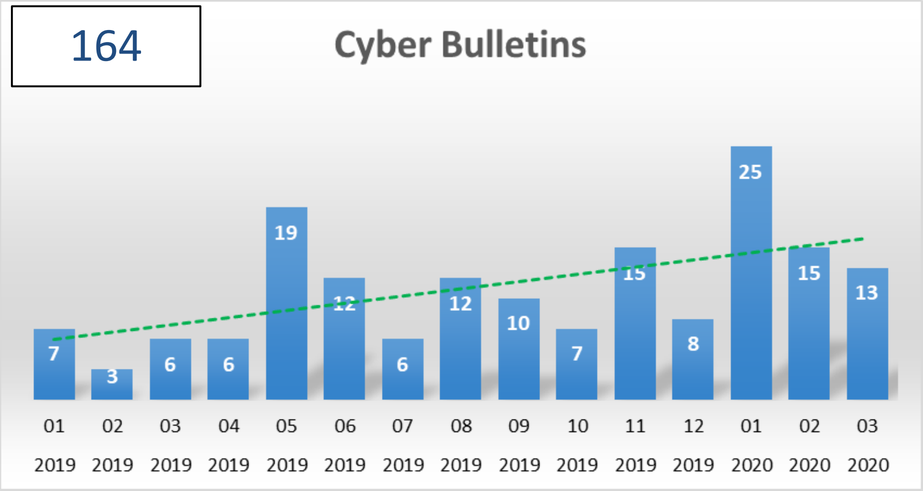
540

Cyber

- 101 unique member organizations had at least one cyber share (Jan’19-Mar’20)
- 9 members had 10 or more shares
- Most sharing came via the Portal, but other channels are increasing in use

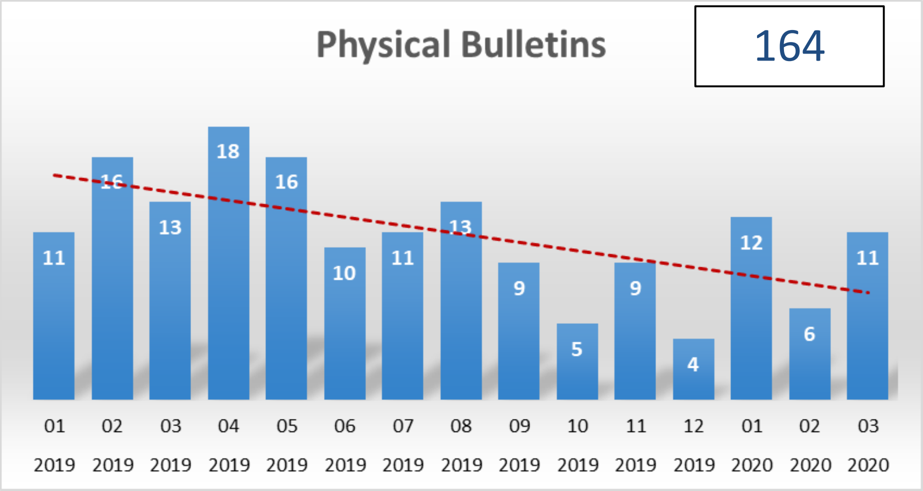
Metrics - Analysis

E-ISAC Staff Portal Postings (Volume)



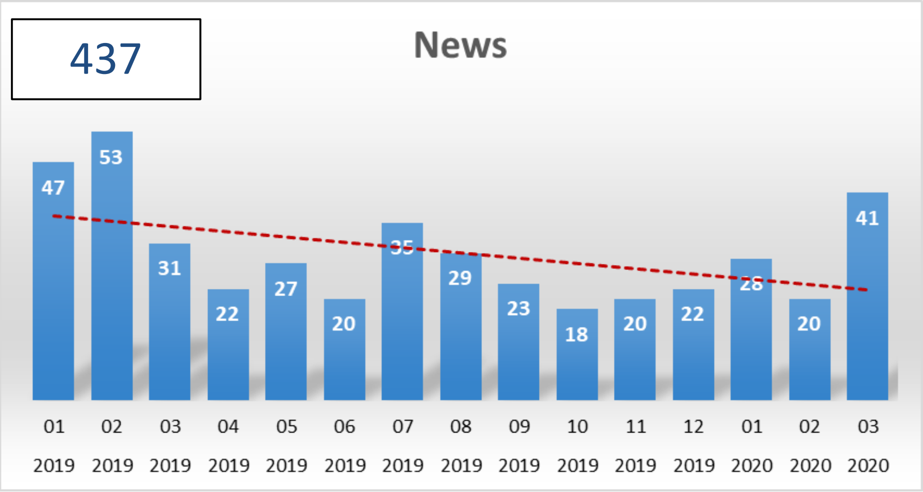
Cyber Bulletins

164



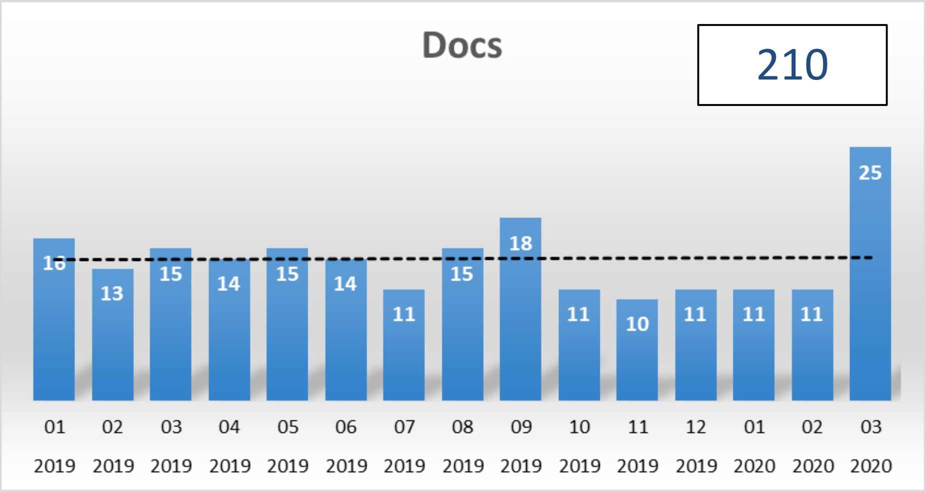
Physical Bulletins

164



News

437



Docs

210

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Preliminary 2021 E-ISAC Budget

Andy Sharp, Vice President, Interim Chief Financial Officer
Technology and Security Committee Open Meeting
May 13, 2020

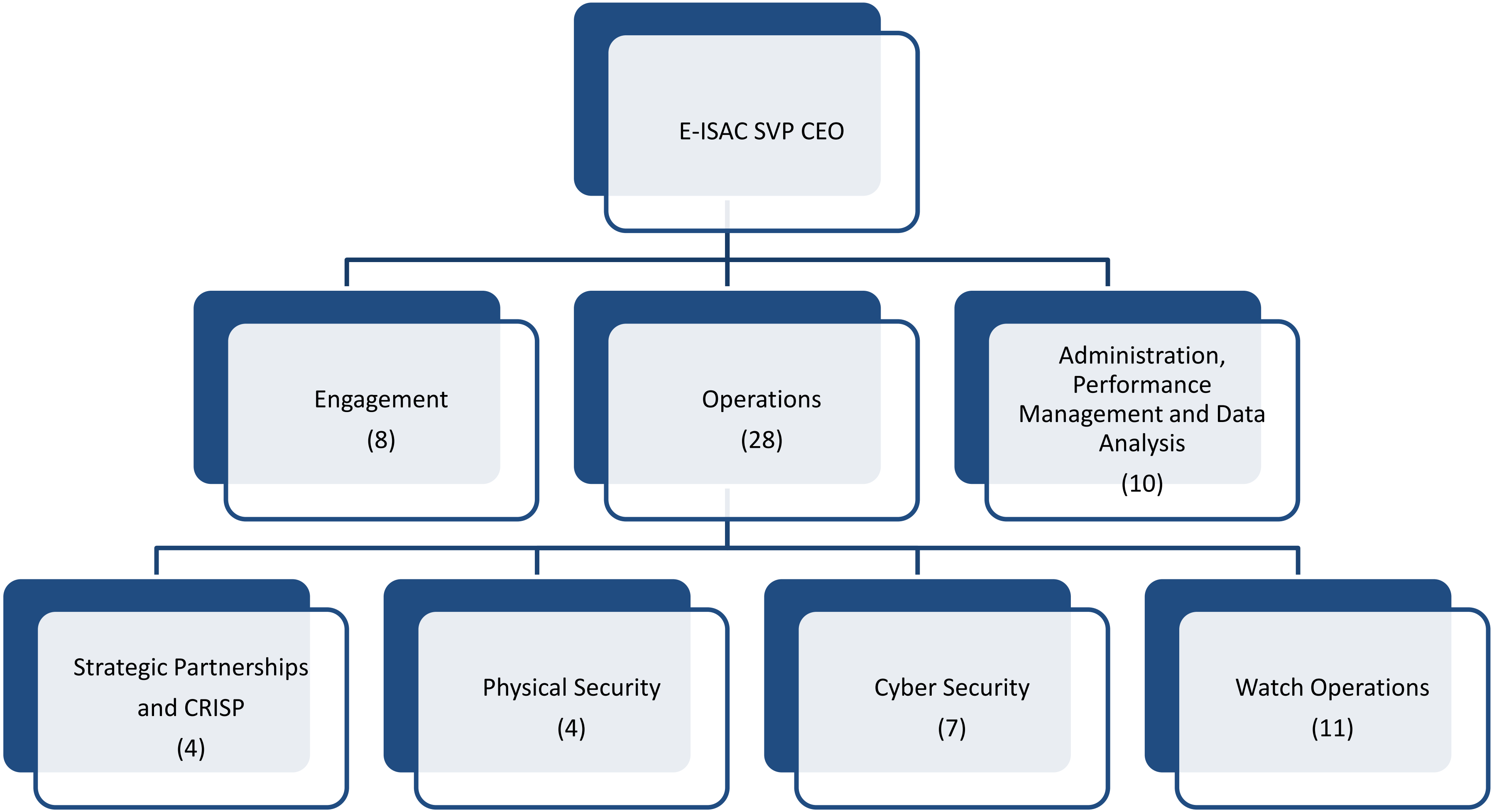
RELIABILITY | RESILIENCE | SECURITY

Budget Performance and 2021 Focus

2019	2020	2021
On budget	On budget (projected)	Below prior projection

- Resource focus (2020-2021)
  - Supporting near-term strategic plan priorities
  - Reduction in projection is not expected to impact current initiatives
  - Mitigating upward resource pressure
    - Ensuring effectiveness and efficiency of operations
    - Maximizing utilization of current staffing, teamwork
    - Leveraging partnerships
    - Effective use of technology to support strategy

E-ISAC Organization Chart



E-ISAC SVP CEO

Engagement
(8)

Operations
(28)

Administration, Performance Management and Data Analysis
(10)

Strategic Partnerships and CRISP
(4)

Physical Security
(4)

Cyber Security
(7)

Watch Operations
(11)

2021 Revised Projection

E-ISAC DIRECT COSTS
2021 Projection --- 2021 Revised Budget Projection

	2021	2021		
	Projection	Revised	$	$
	from 2020 BP&B	Projection	Change	Change
Personnel	$ 11,493,752	$ 9,390,243		
Meetings & Travel	464,200	297,080		
Operating Expenses	9,844,202	9,927,042		
Fixed Assets	671,450	692,880		
Total Direct Costs	$ 22,473,604	$ 20,307,245	$ (2,166,359)	-9.6%
CRISP Portion	$ 8,311,450	$ 7,556,059	$ (755,391)	-9.1%
Non-CRISP Portion	$ 14,162,154	$ 12,751,186	$ (1,410,968)	-10.0%

2021 Revised Projection vs 2020 Budget

E-ISAC DIRECT COSTS

2020 Final Budget --- 2021 Revised Budget Projection

	2020 Final Budget	2021 Revised Projection	$ Change	$ Change
Personnel	$ 9,825,628	$ 9,390,243		
Meetings & Travel	464,200	297,080		
Operating Expenses	9,728,189	9,927,042		
Fixed Assets	421,450	692,880		
Total Direct Costs	$ 20,439,467	$ 20,307,245	$ (132,222)	-0.6%
CRISP Portion	$ 8,103,901	$ 7,556,059	$ (547,842)	-6.8%
Non-CRISP Portion	$ 12,335,566	$ 12,751,186	$ 415,620	3.4%

Summary of 2021 Projections

- Total E-ISAC direct costs including CRISP slightly less than 2020 budget and $2.2M (9.6%) below prior forecast
- E-ISAC direct costs excluding CRISP up $416k (3.4%) over 2020 budget and $1.4M (10.0%) below prior forecast
- Continue to evaluate options to reduce direct costs
- Cybersecurity Risk Information Sharing Program (CRISP)
  - Adjustments for known changes and expected lower PNNL costs
  - Participant costs declining primarily due to additional DOE funding
  - Budget, including operational technology pilot funding, subject to review with participants

Summary of 2021 Projections

- E-ISAC (excluding CRISP) 2021 projection summary – increase of $416k (3.4%) over 2020 budget and $1.4M (10.0%) below prior 2021 projection
  - <u>Personnel</u>:
    - Below prior projection by $2.1M (20%) – lower FTE resources
    - Phased transition of watch contractors to full time employees
    - Ongoing evaluation of watch resource needs
    - Market increases in compensation and benefits
  - <u>Operating Expenses</u>
    - Above prior projection by $823k (32%)
    - Continued contractor support for Watch operations during phased transition
    - Ongoing software, hardware, and contractor costs
    - Resource support for physical security threat workshops

Summary of 2021 Projections

- E-ISAC (excluding CRISP) 2021 projection summary (continued)
  - Fixed Assets
    - Flat with prior projection
    - Data platform, portal, and secure data center investments
  - Meetings, Travel and Conference Calls
    - Decreased by $147k – meetings (30%) and travel (40%)

Next Steps

- **May-June**: Feedback and follow up with Member Executive Committee
- **July 14:** Second draft posted for comment
- **July 21 :** MEC conference call to review final proposed 2021 E-ISAC budget
- **July 23:** FAC webinar to preview second draft
- **August 20:** Final E-ISAC budget presented to NERC Board as part of overall NERC budget

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Business Technology Projects Update

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
May 13, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

- ERO Information Technology Projects Update
  - Centralized Organization Registration ERO System (CORES)
  - Geomagnetic Disturbance (GMD) application
  - Microsoft TEAMS Collaboration Platform
- Electricity Information Sharing and Analysis Center (E-ISAC) Technology Projects
  - Salesforce customer relationship management (CRM)
  - E-ISAC Portal
  - Data Analysis Platform
- Priorities Looking Ahead

CORES

- Rollout to all Regions completed
- Benefits Realization Phase will begin once all entities are on-boarded

CORES:
What to expect as a registered entity?

Registered Entity

Functionality

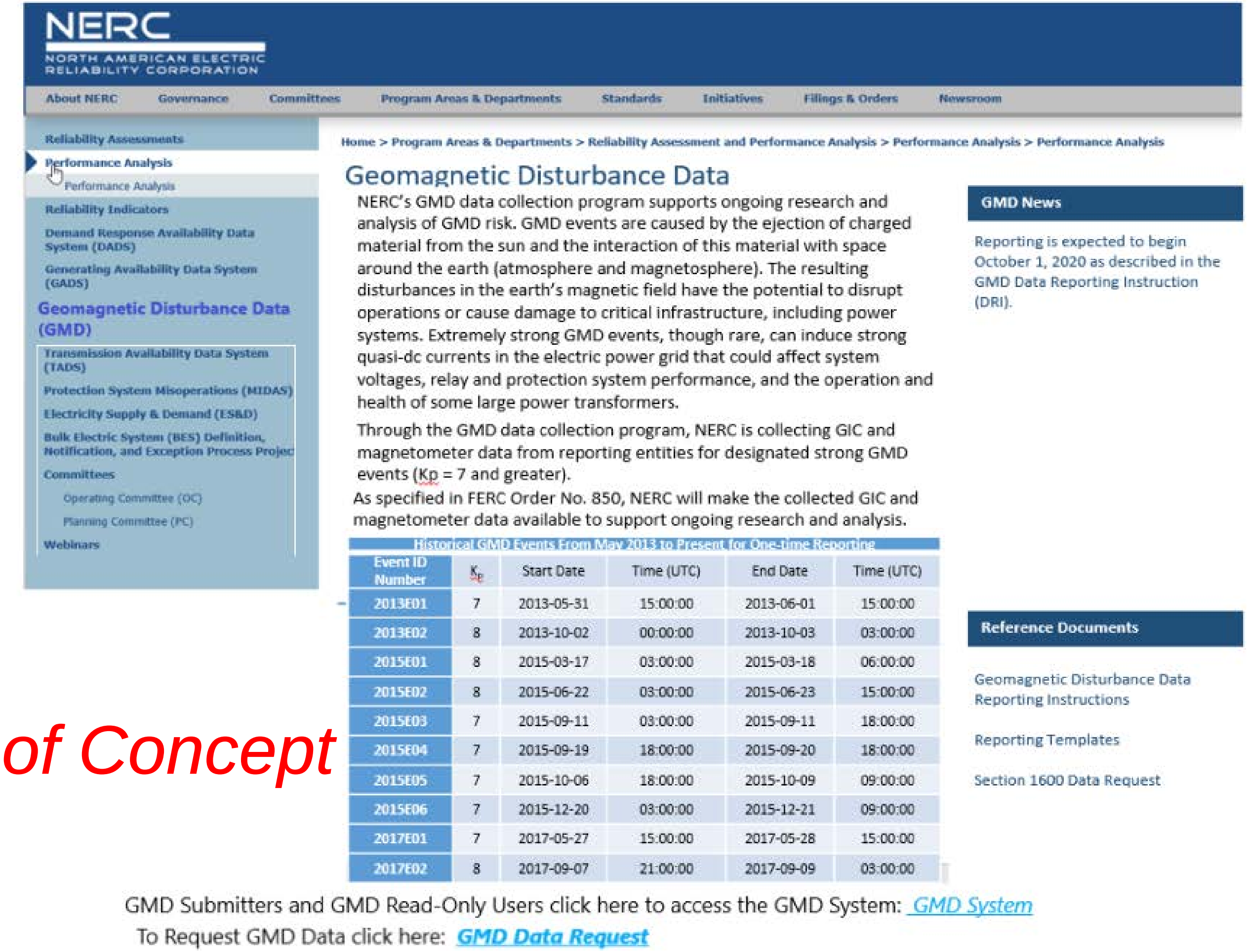
- Create and submit new registration requests
- Receive notifications when new registrations are submitted
- After Regional and NERC approval, manage the newly submitted registration record
- Manage existing registration records (those that exist today in CITS, CDMS, and CRATS)
- Manage contacts for their entity
- Receive notifications when registration changes (including new registrations) are approved
- View Coordinated Oversight Information related to their entity

GMD

- Section 1600 Data Request; FERC Order 830
- Data reporting mechanism for GMD data
- Key users: transmission owners and generator owners
- Developed, hosted and secured by NERC’s xRM platform

GMD

- Stakeholders will have access to GMD data via NERC.com



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
About NERC
Governance
Committees
Program Areas & Departments
Standards
Initiatives
Filings & Orders
Newsroom
Reliability Assessments
Performance Analysis
Performance Analysis
Reliability Indicators
Demand Response Availability Data System (DADS)
Generating Availability Data System (GADS)
Geomagnetic Disturbance Data (GMD)
Transmission Availability Data System (TADS)
Protection System Misoperations (MIDAS)
Electricity Supply & Demand (ES&D)
Bulk Electric System (BES) Definition, Notification, and Exception Process Projec
Committees
Operating Committee (OC)
Planning Committee (PC)
Webinars
Home > Program Areas & Departments > Reliability Assessment and Performance Analysis > Performance Analysis > Performance Analysis

Geomagnetic Disturbance Data

NERC's GMD data collection program supports ongoing research and analysis of GMD risk. GMD events are caused by the ejection of charged material from the sun and the interaction of this material with space around the earth (atmosphere and magnetosphere). The resulting disturbances in the earth's magnetic field have the potential to disrupt operations or cause damage to critical infrastructure, including power systems. Extremely strong GMD events, though rare, can induce strong quasi-dc currents in the electric power grid that could affect system voltages, relay and protection system performance, and the operation and health of some large power transformers.

Through the GMD data collection program, NERC is collecting GIC and magnetometer data from reporting entities for designated strong GMD events (Kp = 7 and greater).

As specified in FERC Order No. 850, NERC will make the collected GIC and magnetometer data available to support ongoing research and analysis.

Historical GMD Events From May 2013 to Present for One-time Reporting

Event ID Number	K_p	Start Date	Time (UTC)	End Date	Time (UTC)
2013E01	7	2013-05-31	15:00:00	2013-06-01	15:00:00
2013E02	8	2013-10-02	00:00:00	2013-10-03	03:00:00
2015E01	8	2015-03-17	03:00:00	2015-03-18	06:00:00
2015E02	8	2015-06-22	03:00:00	2015-06-23	15:00:00
2015E03	7	2015-09-11	03:00:00	2015-09-11	18:00:00
2015E04	7	2015-09-19	18:00:00	2015-09-20	18:00:00
2015E05	7	2015-10-06	18:00:00	2015-10-09	09:00:00
2015E06	7	2015-12-20	03:00:00	2015-12-21	09:00:00
2017E01	7	2017-05-27	15:00:00	2017-05-28	15:00:00
2017E02	8	2017-09-07	21:00:00	2017-09-09	03:00:00

GMD News

Reporting is expected to begin October 1, 2020 as described in the GMD Data Reporting Instruction (DRI).

Reference Documents

Geomagnetic Disturbance Data Reporting Instructions

Reporting Templates

Section 1600 Data Request

GMD Submitters and GMD Read-Only Users click here to access the GMD System: GMD System

To Request GMD Data click here: **GMD Data Request**

Proof of Concept

Microsoft TEAMS

- Unified communications and collaboration platform
- Enables secure remote collaboration
- Access, share and edit documents, PowerPoints and spreadsheets
- Strategic investment for NERC, ERO Enterprise and registered entities in a post-coronavirus world

E-ISAC

- CRM tool (Salesforce) in production, saving time and increasing the accuracy of member tracking and stakeholder contacts
- E-ISAC Portal – Platform upgrade completed in April; additional refinements underway; focus on content publication (actionable information)
- E-ISAC Data Platform – Pilot release occurred April 1; build out occurring with a heavy focus on data interfaces and data sharing, which will enable additional improved analytics and information sharing for watch operations, analysts and data scientist teams

Priorities Looking Ahead

- Analytical capabilities for the E-ISAC
- Accelerated adoption of Salesforce capabilities for the E-ISAC
- Implementation of Microsoft Teams
- Various software/hardware upgrades to NERC infrastructure

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Align Project Update

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
May 13, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Align Benefits
- Align Release 1
- How To Stay Informed
- Current Status
- Align Release 2 and Release 3 Functionality

Align - Benefits

Moving to a common platform will provide:

- Alignment of **common** Compliance Monitoring & Enforcement Program (CMEP) **business processes**, ensuring consistent practices and data gathering
- A **standardized interface** for registered entities to interact with the ERO Enterprise
- **Real-time access to information**, eliminating delays and manual communications
- **Consistent application** of the CMEP
- **More secure** method of managing and storing CMEP data

Align Release 1:
What to expect as a registered entity?

Stakeholder Group

Registered Entities

Release 1 Functionality

- Create and submit Self-Reports and Self-Logs
- Create and manage mitigating activities (informal) and Mitigation Plans (formal)
- View and track Open Enforcement Actions (EAs) resulting from all monitoring methods
- Receive and respond to Requests for Information (RFIs)
- Receive notifications and view dashboards on new/open action items
- Generate report of Standards and Requirements applicable to your entity
- Manage user access for your specific entity

Align Release 1:
What to expect as a Regional Entity?

Stakeholder Group

Regional Entities

Release 1 Functionality

- Receive Self-Reports and Self-Logs from entities
- Manually create findings that result from any monitoring method (Audits, Spot Checks, Investigations, PDSs, Self-Certifications, Complaints)
- Perform Preliminary Screens, Potential Noncompliance Reviews, and disposition determinations for each PNC/EA
- Send and received responses to RFIs
- Trigger notifications such as Notice of Alleged Violation(s) and Proposed Penalty or Sanction, Notices of Confirmed Violation(s), Compliance Exception Letter(s), Find, Fix, Track & Report Letter(s), and Settlement Agreements
- Receive, review, and approve mitigating activities (informal) and Mitigation Plans (formal)
- Receive notifications and view dashboards on new/open action items
- Generate report of Standards and Requirements applicable to a registered entity

Align Release 1:
What to expect as NERC?

Stakeholder Group

NERC Users

Release 1 Functionality

- Perform oversight of the activities of Regional Entities
- View dashboards on new/open action items
- Create reports required by FERC related to Enforcement and Mitigation activities
- Generate report of Standards and Requirements applicable to a registered entity

How To Stay Informed

Key communication vehicles

- Align newsletter for Regions and registered entities
- Regional Change Agent Network
- Dedicated project page on NERC.com: Click Here
- Upcoming CMEP Regional workshops
- Trades meetings, as appropriate

Upcoming Milestones

- Process re-harmonization including ERO Secure Evidence Locker (SEL)
- Training videos for Release 1
- User guides and quick reference cards
- Regional adoption workshops
- Change agent preparations
- Functional design for Release 2

Align Future Releases: What to expect?

Release 2 Functionality Est. 2021

- Technical Feasibility Exceptions
- Periodic Data Submittals
- Self-Certifications

Note: A strategy is being developed for how these monitoring methods will be managed in the gap between Releases

Release 3 Functionality Est. 2021

- Compliance Planning (Risk, CMEP Implementation Plan, Inherent Risk Assessment, Internal Controls Evaluation, Compliance Oversight Plan)
- Compliance Audit
- Spot Check
- Compliance Investigations
- Complaints

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Establishment of the ERO Enterprise Secure Evidence Locker

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
May 13, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Problem Statement
- Solution Overview
  - Guiding Principles
  - ERO Enterprise Secure Evidence Locker (ERO SEL) Overview
  - NIST Standard
  - Project Justification
- Potential Risks

Problem Statement

- Issues Discovered:
  - Inconsistent processes for requesting, handling and storage of evidence
  - Critical data protection requires additional capabilities beyond our current systems
  - Critical data protection is and will remain a CEO-level concern for our industry, hence the “gold standard” expectation
- Recommended Solution:
  - Provides content separation in connection with CMEP activities
  - Create a highly secure ERO Enterprise evidence locker
  - Harmonize processes for evidence collection processes
  - Enhance ERO Enterprise work products to reduce risk of a critical data exposure
  - Conduct independent review prior to launch and prior to new releases

Design Principles

- All registered entity provided evidence* will go into the registered entity or ERO SEL (any registered entity locker must meet certain criteria the ERO Enterprise develops for functionality, access, etc.)
- ERO Enterprise workflow and work products will be in the ERO Enterprise Align Tool
- The ERO Enterprise will enhance ERO Enterprise work products (e.g., working papers) to support conclusions without the need to store data for extended periods, minimizing a data protection risk

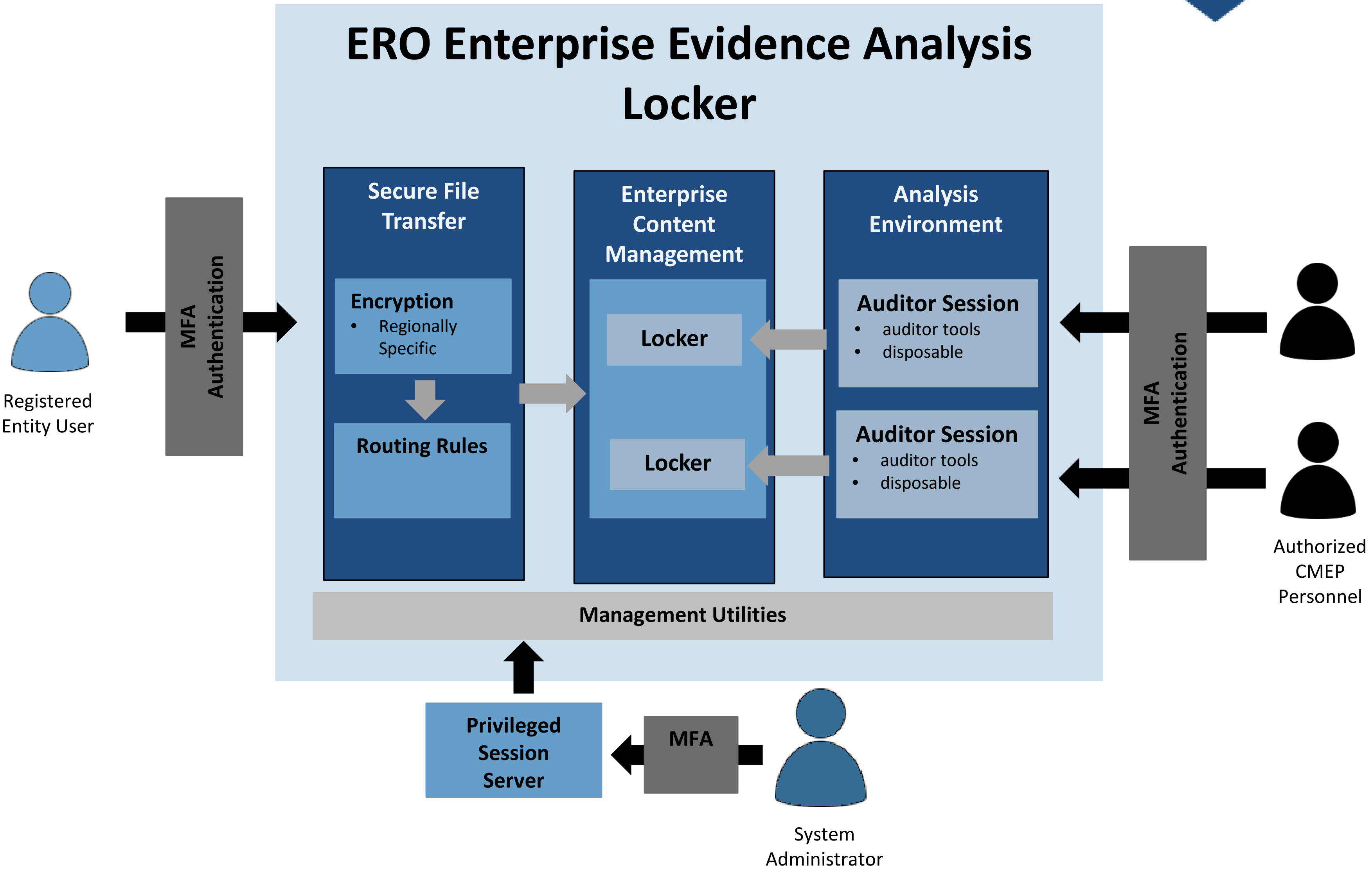
**Unless prohibited by a standard*

NOTE: Achieving this will occur via training, guidance, oversight activities and other outreach channels

What is the ERO SEL?

- A highly secure, isolated environment
  - Purpose-built to collect and protect evidence
  - Enables submission by authorized and authenticated entity users
  - Provides compartmentalized analysis of evidence in temporary, isolated, disposable environments
  - No interfaces with any other systems
- Evidence
  - Is encrypted immediately upon submission
  - Is securely isolated per entity
  - Is never extracted
  - Is never backed up
  - Is subject to proactive and disciplined destruction policies

ERO SEL - How will it work? Technical Implementation



NIST Standard

- NIST 800-171 contains 110 controls in 14 key areas including:
  - Access Control
  - Physical Protection
  - System and Information Integrity
  - Personnel Security
  - Incident Response
  - Risk Assessment

ERO SEL Project Justification

- Significantly reduces risk for evidence loss and exposure
- Solution design informed by stakeholder input
- Allows content segregation to significantly enhance security
- Highest commercially available design to conform to NIST 800.171 standard ("the gold standard")

ERO SEL Potential Risks

- Required NERC Board and regulatory approvals
- Licensing of new technologies
- Support of new technologies
- Delays created by the coronavirus pandemic
  - Potential supply chain delays (hardware)
  - Professional Services (travel and collaboration)
  - Testing and in-person training

Questions and Answers