A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Operations and Strategic Plan Update

Manny Cancel, NERC SVP and CEO of the E-ISAC

Technology and Security Committee Meeting

August 19, 2020

TLP:GREEN

RELIABILITY | RESILIENCE | SECURITY

Agenda

- E-ISAC Operations Update
  - COVID-19 Operations
  - Threat Landscape
  - Operations Update
  - Information Sharing
  - Member Feedback
  - Strategic Partnerships
- E-ISAC Strategic Plan – Review and Endorsement

COVID-19 Operations

- Actively tracking COVID-19 since February 2020
  - Activated business continuity plan and continue to work remotely
  - Provide daily COVID-19 awareness reporting and threat intelligence
  - Participate in Electricity Subsector Coordinating Council (ESCC) activities
    - Regular update calls with industry and government
    - Tactical Tiger Teams
    - Tri-sector efforts
  - Coordinate with broader cross-sector community on response activities and updates

Threat Landscape

Cyber

- Geopolitical and state-sponsored attacks
- Ransomware attacks
- Attacks exploiting vulnerabilities in collaboration and other corporate software platforms
- COVID-19-related disinformation and malware campaigns

Physical

- Increase in intrusion, vandalism, and gunfire-related incidents
- Activist and protest activity
- Increased surveillance activities using unmanned aircraft systems (drones)
- E-ISAC reports and products released

Operations Update

- 24x7 Watch is fully operational
- Membership has increased by 10% in 2020
- New member onboarding processes and products
- GridEx VI – vendor selected and contract negotiations underway
- Cybersecurity Risk Information Sharing Program (CRISP)
  - Revised CRISP Governance Committee Charter and Data Handling Guide
  - Sys log pilot deployed to two utilities and will be extend to six more by Q4 2020
  - CRISP Operational Technology (OT) pilot recommendation pending additional discussions with Department of Energy (DOE) and CRISP participants

Information Sharing
Through July 31

E-ISAC

Through July 31, 2020	News Items	Cybersecurity Bulletins	Physical Security Bulletins	Reports and Reference Documents	Events
24x7 Watch	207	9	2	124	2
Cyber Threat Intelligence Team	25	89	0	2	0
Physical Security Analysis Team	25	0	62	26	1
Engagement	7	0	0	24	10
Other	0	5	0	2	0
Totals	**264**	**103**	**64**	**178**	**13**

Member Shares

- Cyber – 356
- Physical Security – 542 (through June 30)

Member Feedback

- Feedback on E-ISAC events, products, and services is generally positive and informs direction
- Use of electronic feedback facilities is limited
- Regular sources of feedback include:
  - **Industry Engagement Program** – 100% participation and 80% excellent rating
  - **GridSecCon** – 85% satisfaction; feedback reinforced value of networking (4.43/5 stars) and training opportunities (84% participation)
  - **GridEx** – 94% of participants said that GridEx allowed them to exercise their Operational Response Plans “Very Well” or “Well”
  - **Portal Postings** – Low response rate (10% response using rating system and 16% of postings receive comments)

Member Feedback

Next Steps

- Gather more input on the quality and content of information shares by members and the E-ISAC
  - Apply industry best practices to gather and manage feedback
  - Use customer relationship management tool to enable more effective reporting and analysis
  - Streamline and optimize use of survey platforms
  - Conduct comprehensive survey in Q1 2021

Strategic Partnerships

- Facilitate enhanced government-industry collaboration
  - Leverage DOE resources
  - Leverage Department of Homeland (DHS) Security Cybersecurity Infrastructure and Security Agency intelligence products
- Multi-State ISAC, Downstream Natural Gas ISAC
  - Co-authored “Current Trends in Ransomware for Utilities”
  - Participating in E-ISAC monthly webinars
- Independent Electricity System Operator (IESO)
  - Monthly analyst-to-analyst sharing of threat and vulnerability information
  - Collaboration with U.S. and Canadian Intelligence Communities on OT analytic frameworks (e.g., MITRE ATT@CK)
  - Continuing to explore opportunities with CRISP and Project Lighthouse
  - IESO Annual Cybersecurity Executive Briefing November 2-3, 2020

A DIVISION OF NERC

E-ISAC

ELECTRICITY
INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Strategic Plan

Manny Cancel, NERC SVP and CEO of the E-ISAC
Technology and Security Committee Meeting
August 19, 2020

TLP:GREEN

RELIABILITY | RESILIENCE | SECURITY

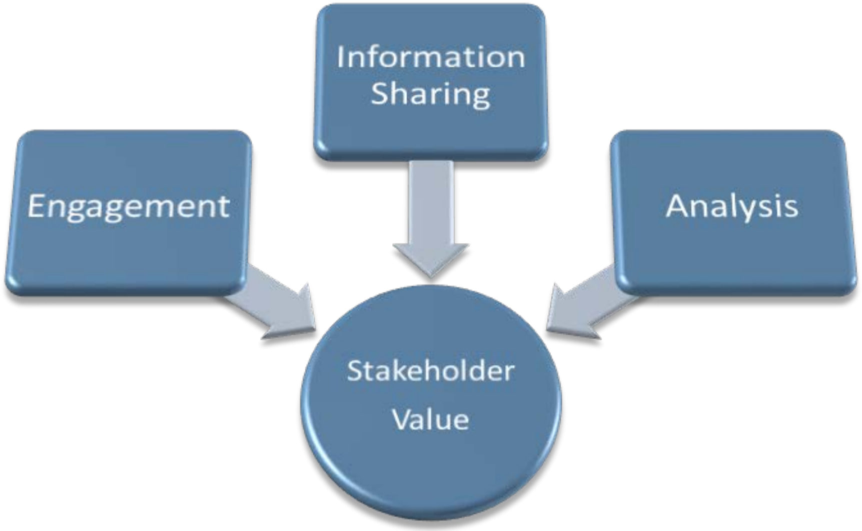
Agenda

- Long-Term Strategic Plan
  - E-ISAC focus
  - Refinements to April draft
  - Resource Plan
  - Member Engagement
  - Partnerships
  - CRISP OT Pilot
  - Technology
- Endorsement of updated Strategic Plan

E-ISAC Focus

Focus areas and objectives remain unchanged

- Providing members with timely and actionable information
- Value-added analysis on security threats and mitigation strategies
- Facilitating collaboration among industry, U.S. and Canadian government partners, and other stakeholders
- Continuous improvement and alignment across our three strategic pillars



Refinements to April Draft

- No significant changes
- Refinements
  - Recognizes E-ISAC role and value in supporting both the ESCC and key government agencies
  - Acknowledges member service needs vary and importance of ongoing stakeholder guidance
  - Clarifies intelligence role as leveraging government and private sector threat and intelligence information (rather than performing an intelligence function)
  - Highlights considerations for evaluating extending services to downstream natural gas sector

Resource Plan

- Maximize use and effectiveness of existing resources
  - No significant personnel increases in 2021 or projected over near term
- Prioritize and ensure value from strategic relationships
- Define role regarding OT initiatives
- Invest in cost effective technology solutions
- Factors that could affect future resource requirements
  - Increased information sharing
  - Large scale OT initiative
  - Extending services to other organizations

Member Engagement

- Additional engagement opportunities
  - Expand and diversify outreach to include smaller and mid-size utilities
  - Collect and respond to member feedback
  - Participate in online speaking engagements
- Enhance new member onboarding experience
  - Implement Designated Approving Official and deploy new member guide
- Promote information sharing
  - Provide members with specific guidance to enhance information sharing
  - Promote 24x7 security operations staffing
  - Showcase analytical products and other tools

Partnerships

- Partnership goals
  - Align goals and strategies to provide timely, actionable information
  - Facilitate enhanced intelligence between government and industry
  - Collaborate on OT security initiatives
- COVID-19 has required us to reprioritize our efforts and timelines with our key partnerships
  - Limited availability of personnel
  - Challenges conducting classified briefings
- Align with National Infrastructure Advisory Council and Cyberspace Solarium recommendations

CRISP OT Pilot

- Objective:
  - Capture raw and refined (i.e., analyzed) OT data, compare to CRISP data, generate processes and playbooks to address threats and vulnerabilities identified in OT and IT data
- Proposals received from Dragos, Pacific Northwest National Lab, and National Rural Electric Cooperative Association/Essence
  - All proposals are technically feasible but offer different features, cost models and implementation challenges
  - Several discussions with CRISP Governance Committee and DOE have taken place
- E-ISAC Recommendation:
  - While significant progress has been made, the E-ISAC recommends a 60 day pause to continue discussions with DOE and CRISP Governance Advisory Committee to finalize recommendation

Technology

- Investments to improve the efficiency of operations, enhance analytical capabilities, and member services
    - Data platform enhancements
    - Portal efficiency enhancements, including Salesforce integration work
- ThreatConnect enrichment (Threat Intelligence Platform)
- Open source information gathering tools (Recorded Future and Dataminr)
- Automated data integration pilot

Questions and Answers

Performance Metrics

Metrics – Engagement
YTD through July 2020

2020 New Users:

1,076

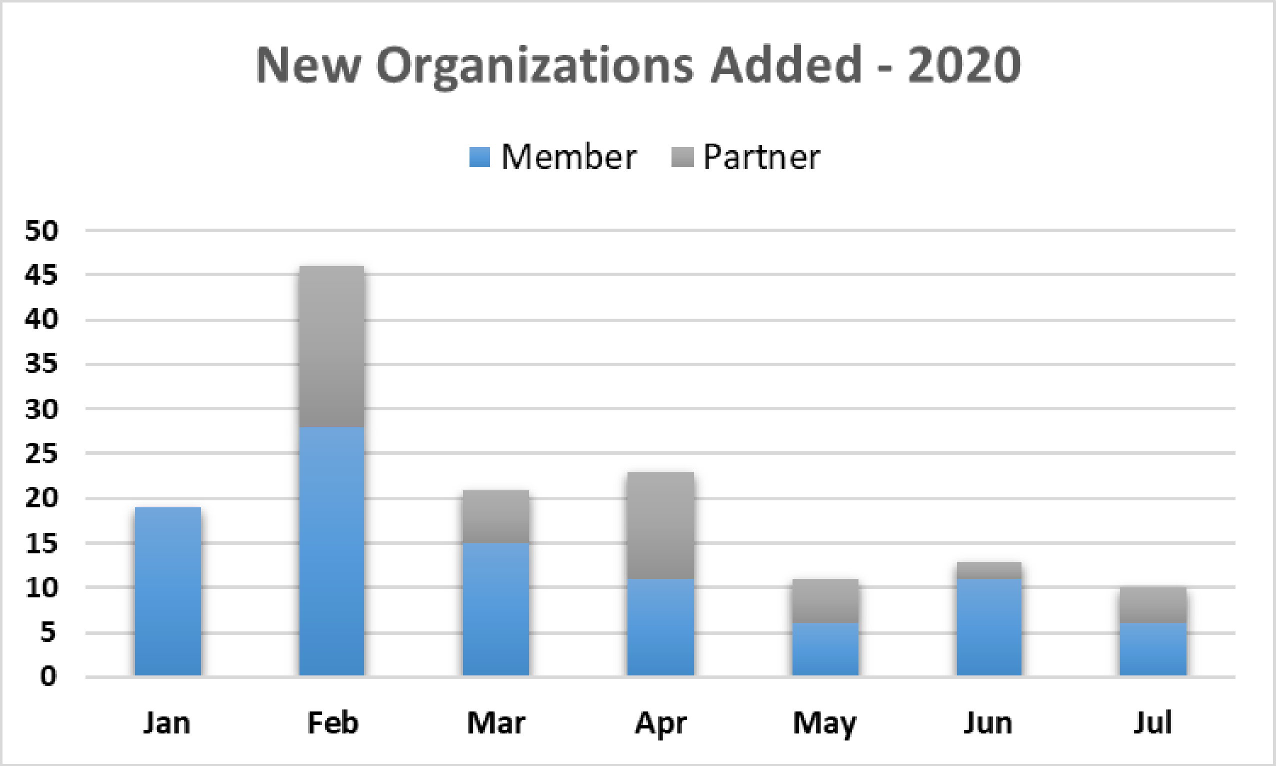
2020 New Organizations:

143

96 Members; 47 Partners

Industry Mix:

Cooperatives added at fastest rate during first half of 2020.



Type	Count	Pct
Cooperative	36	38%
Investor-Owned	23	24%
Other	16	17%
State/Municipality	13	14%
Merchant	4	4%
Federal/Provincial	4	4%

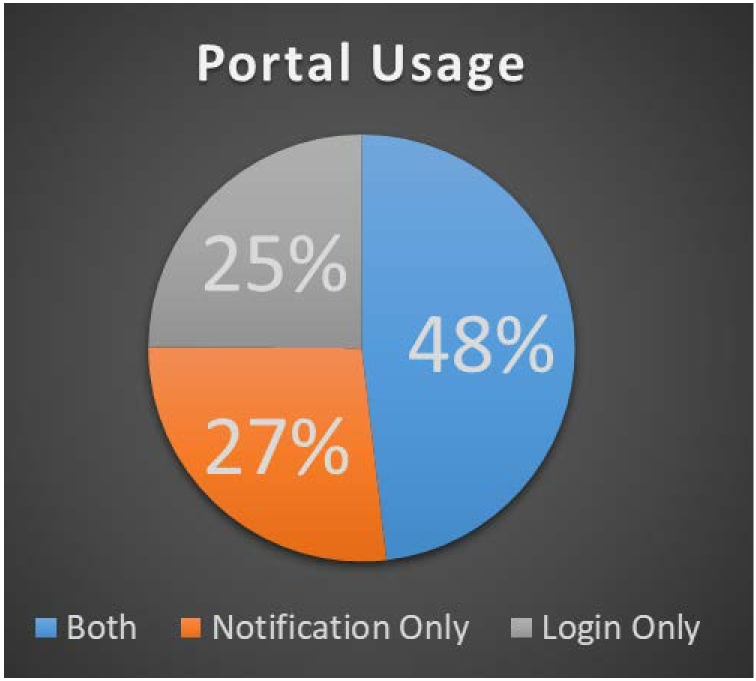
Percent of new Member Orgs

Metrics – Engagement
YTD through July 2020

Jan – Jul 2020 Summary

Sharing from members is still highly concentrated

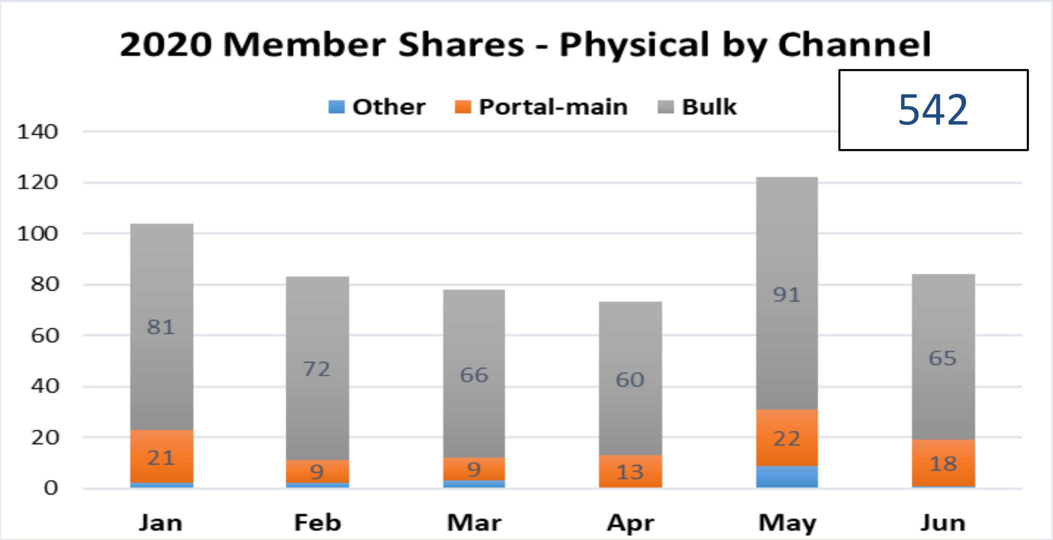
- 79 unique organizations posted at least one share in the first half of 2020
- 72% of all shares came from ten organizations



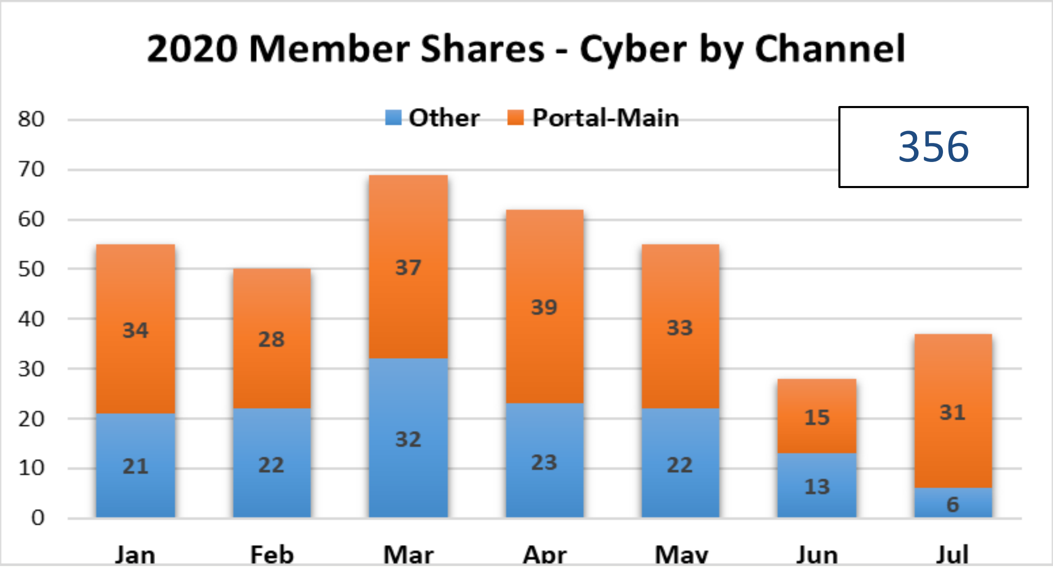
Use of shared information is wider

- 4,820+ users have logged in during 2020 or are currently receiving notifications, representing 1,003+ member organizations (or 75% of total member base of 1,300+ organizations)
- 47% of users have logged in during the last 30 days

Information Sharing – Members



2020 Member Shares - Physical by Channel



2020 Member Shares - Cyber by Channel

Physical (2020 through June)

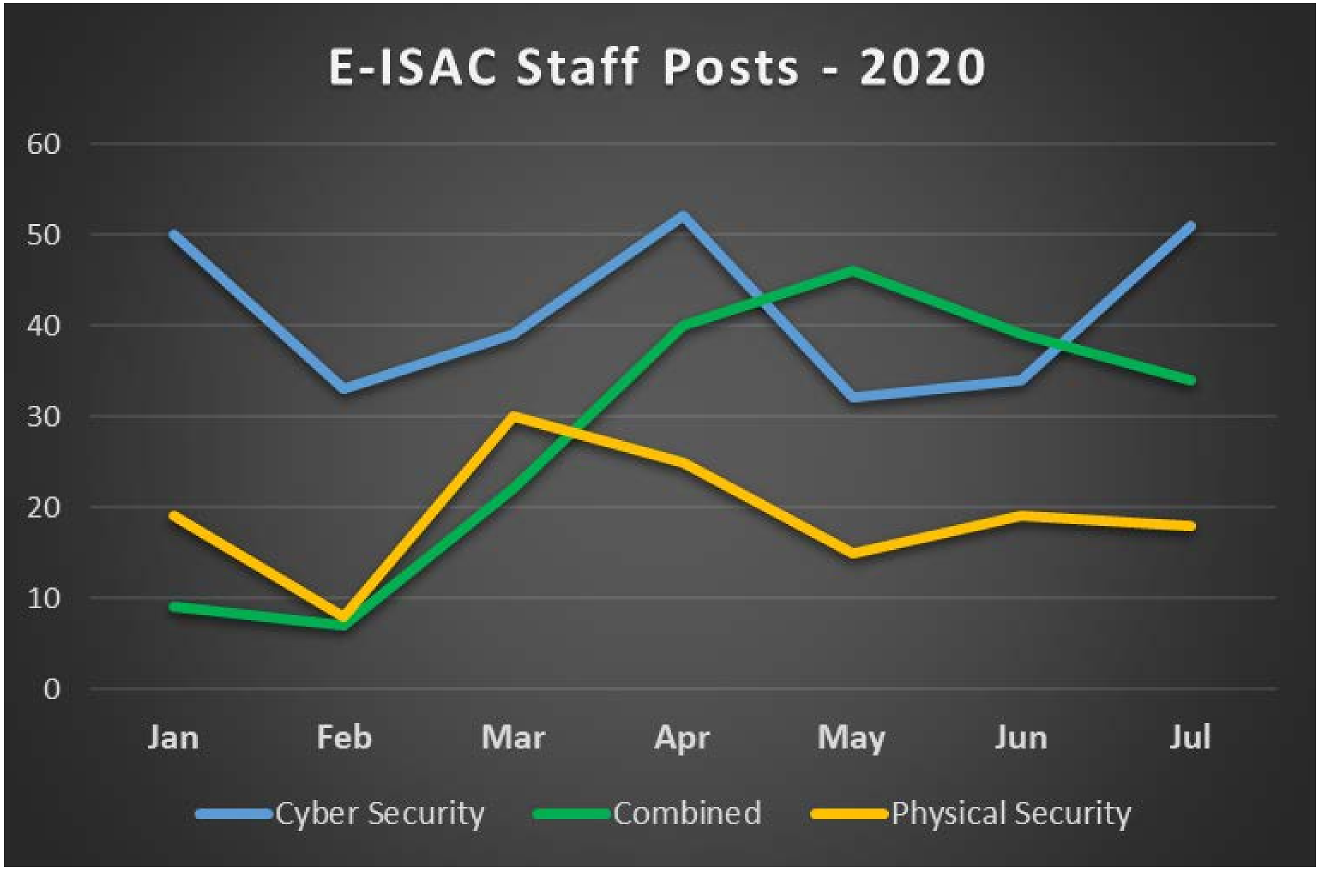
- 44 unique member organizations had at least one physical share
- 81% of all shares came from three members
- 80% shared via bulk channel

Cyber (2020 through July)

- 78 unique member organizations had at least one cyber share
- Six members had 10+ shares and account for 53% of shares
- Most sharing came via the Portal, but top sharers tend to use another channel

Information Sharing – E-ISAC

YTD through July 2020



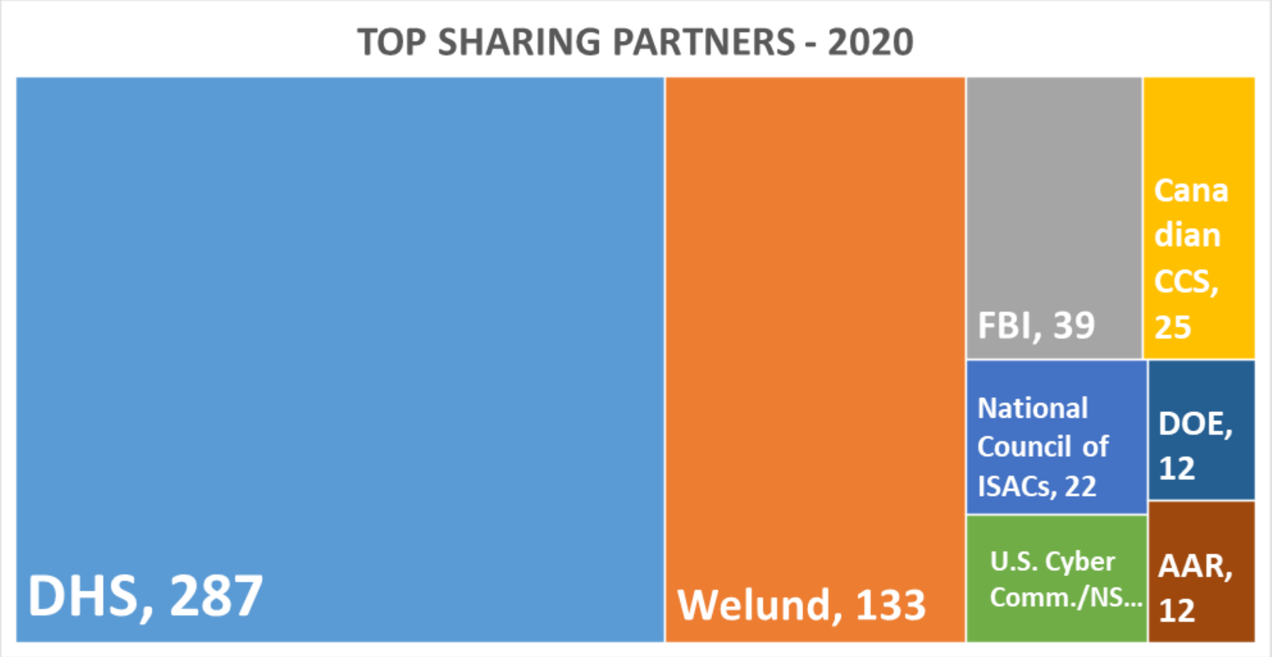
622 total posts in Jan-Jul 2020.

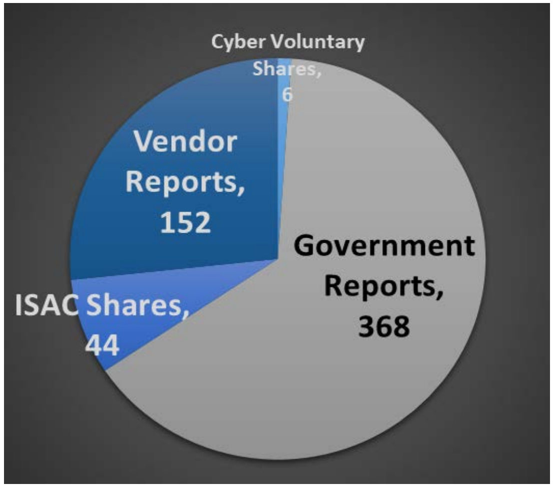
- 291 Cyber
- 197 Combined
- 134 Physical

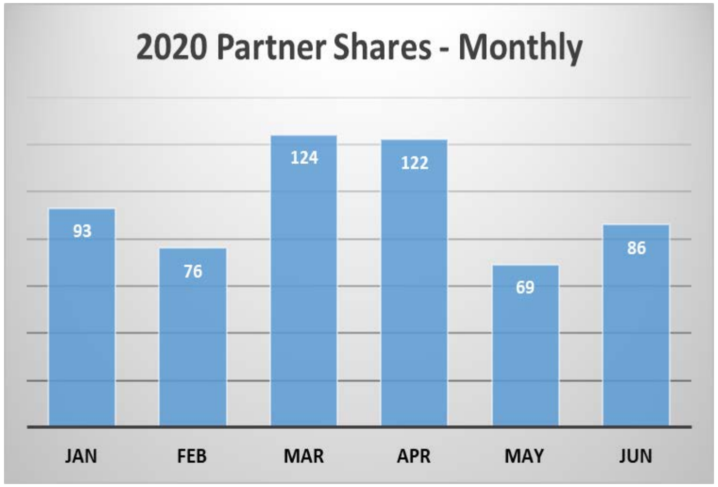
- 177 related to COVID (across Cyber, Combined, and Physical)

Information Sharing-Partners

YTD through June 2020


TOP SHARING PARTNERS - 2020



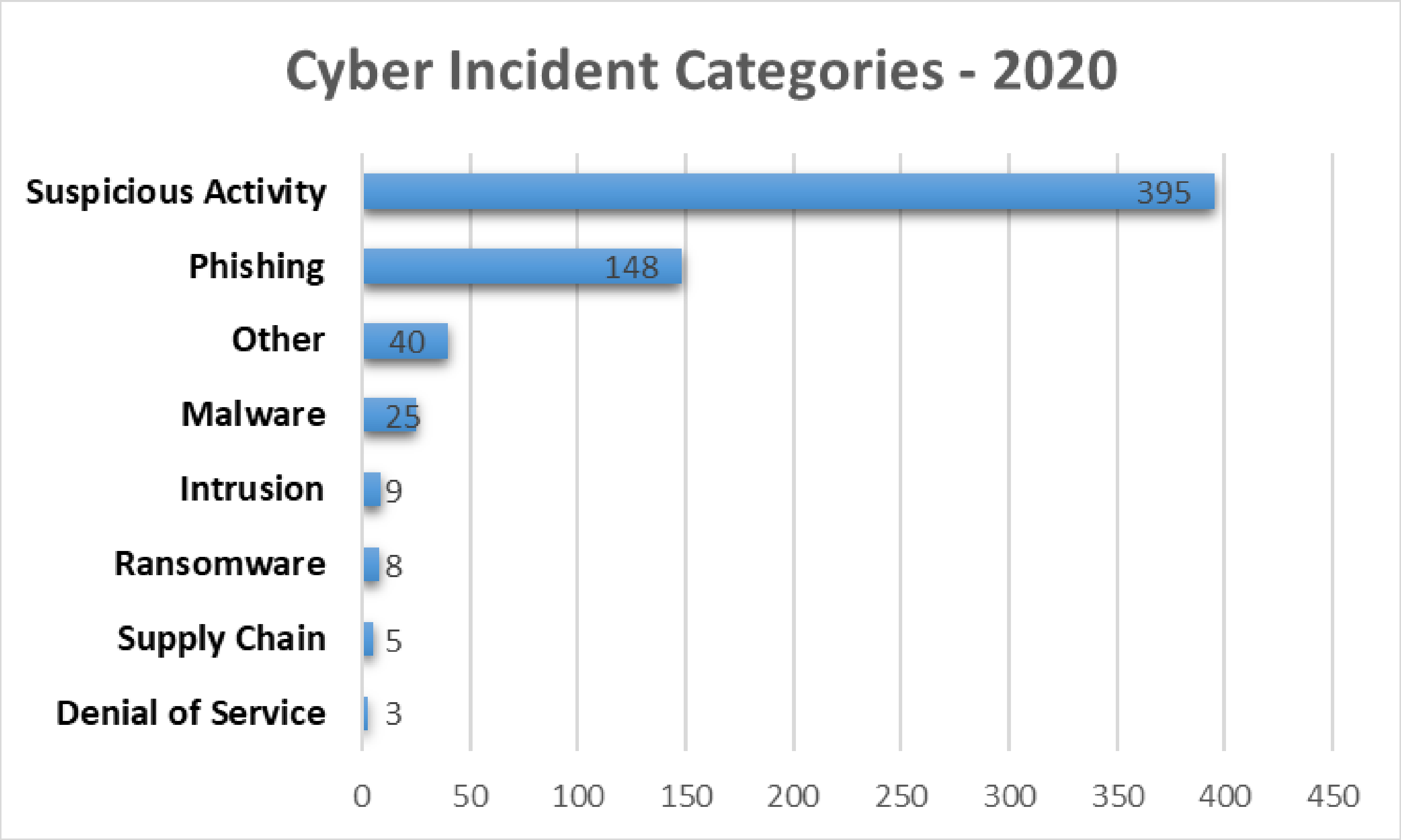

2020 Partner Shares - Monthly

570 total partner posts in first half of the year.

- All come in via other (non-Portal) channels
- Government and vendor reports are most prevalent
- DHS is leading source

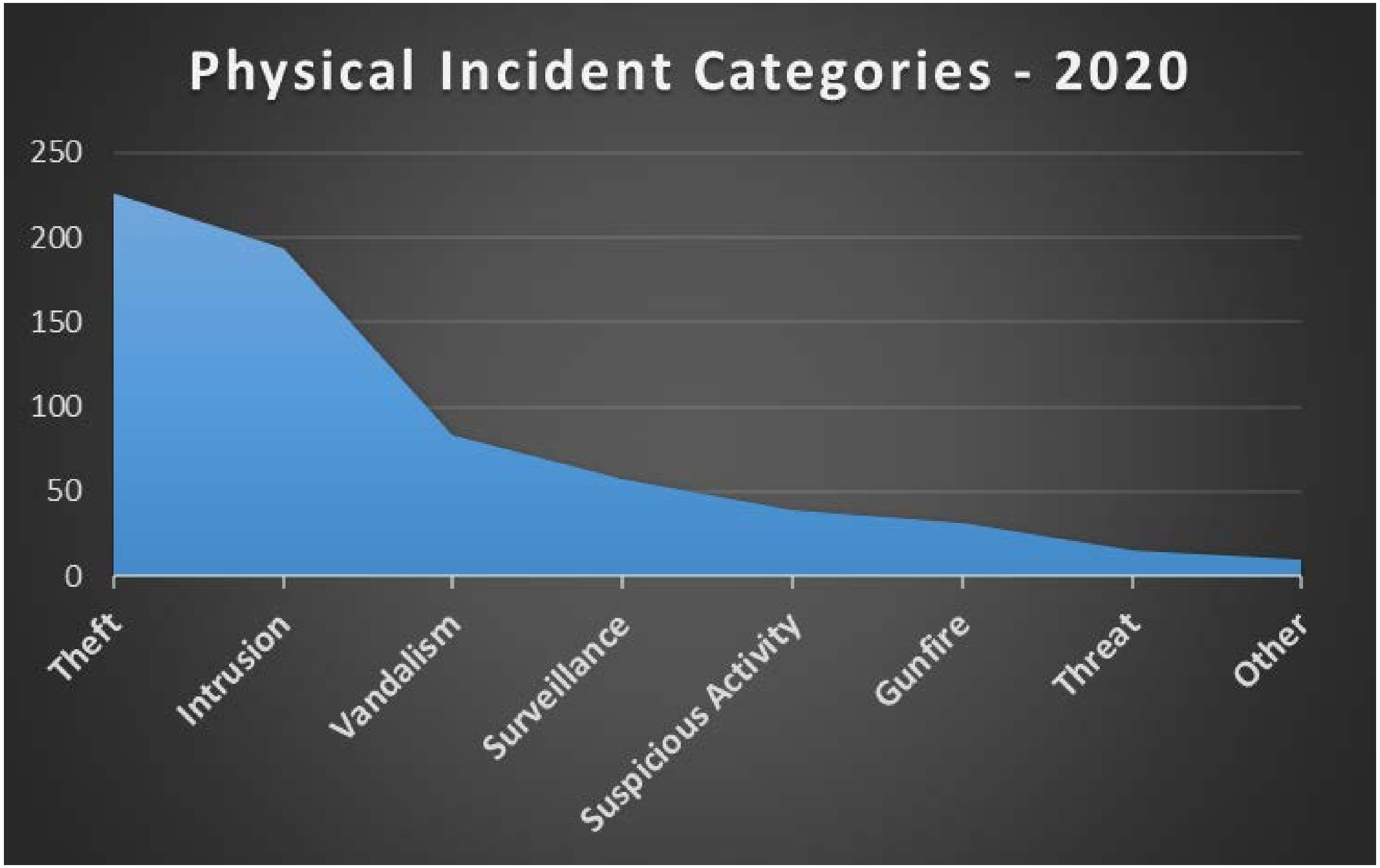
Analysis

YTD through July 2020



- Includes all sources (Member, Partner, E-ISAC)
- Includes Cyber Bulletins, News, and Documents
- Phishing and Suspicious Activity continue to be most frequently reported

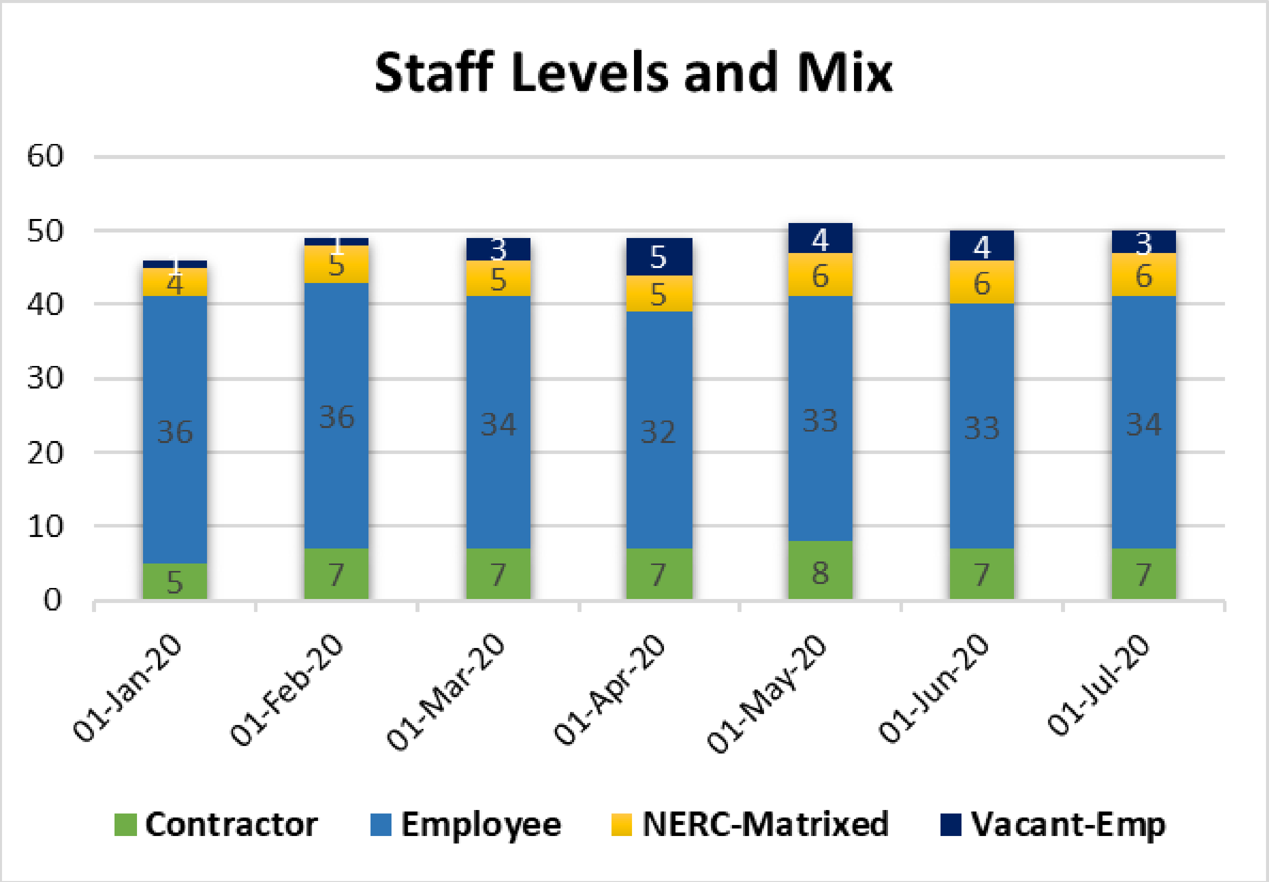
Analysis
YTD through July 2020



- Includes all sources (Member, Partner, E-ISAC)
- Highly concentrated reporting (81% of the above came from three firms)

Workforce

YTD through July 2020



- E-ISAC employees (including vacancies) holding steady at 37, with total staff (including matrixed and contractors) at the 50 mark.
- There are three E-ISAC employee vacancies as of June 30.

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Business Technology Projects Update

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
August 19, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

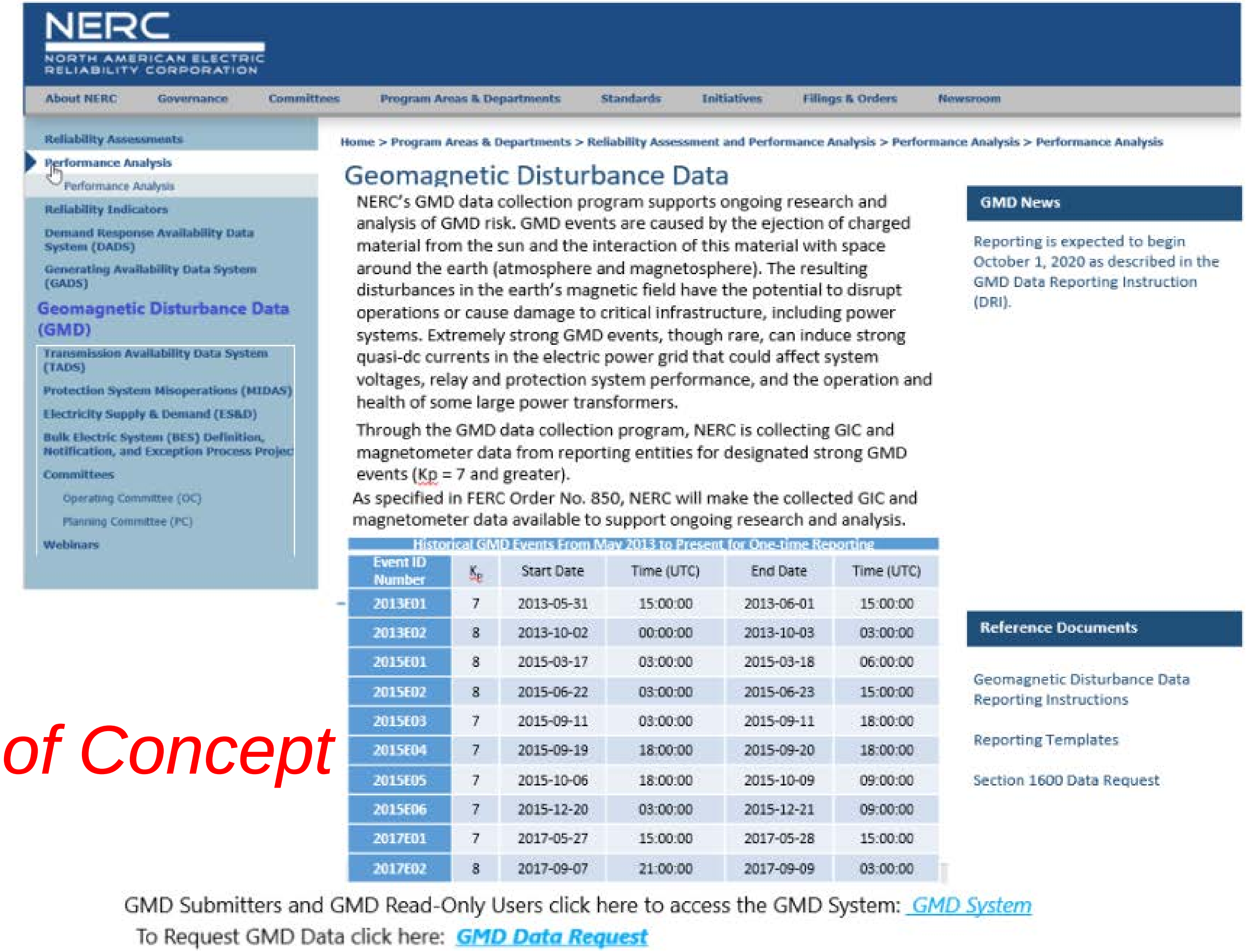
- ERO Business Technology Projects Update
    - Geomagnetic Disturbance (GMD) application
    - Microsoft TEAMS Collaboration Platform
- Electricity Information Sharing and Analysis Center (E-ISAC) Technology Projects
    - Salesforce customer relationship management (CRM)
    - Data Analysis Platform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

GMD

- Section 1600 Data Request; FERC Order 830
- Planned release date of October 1, 2020
- 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 Submitters and GMD Read-Only Users click here to access the GMD System: GMD System

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

GMD News

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

Reference Documents

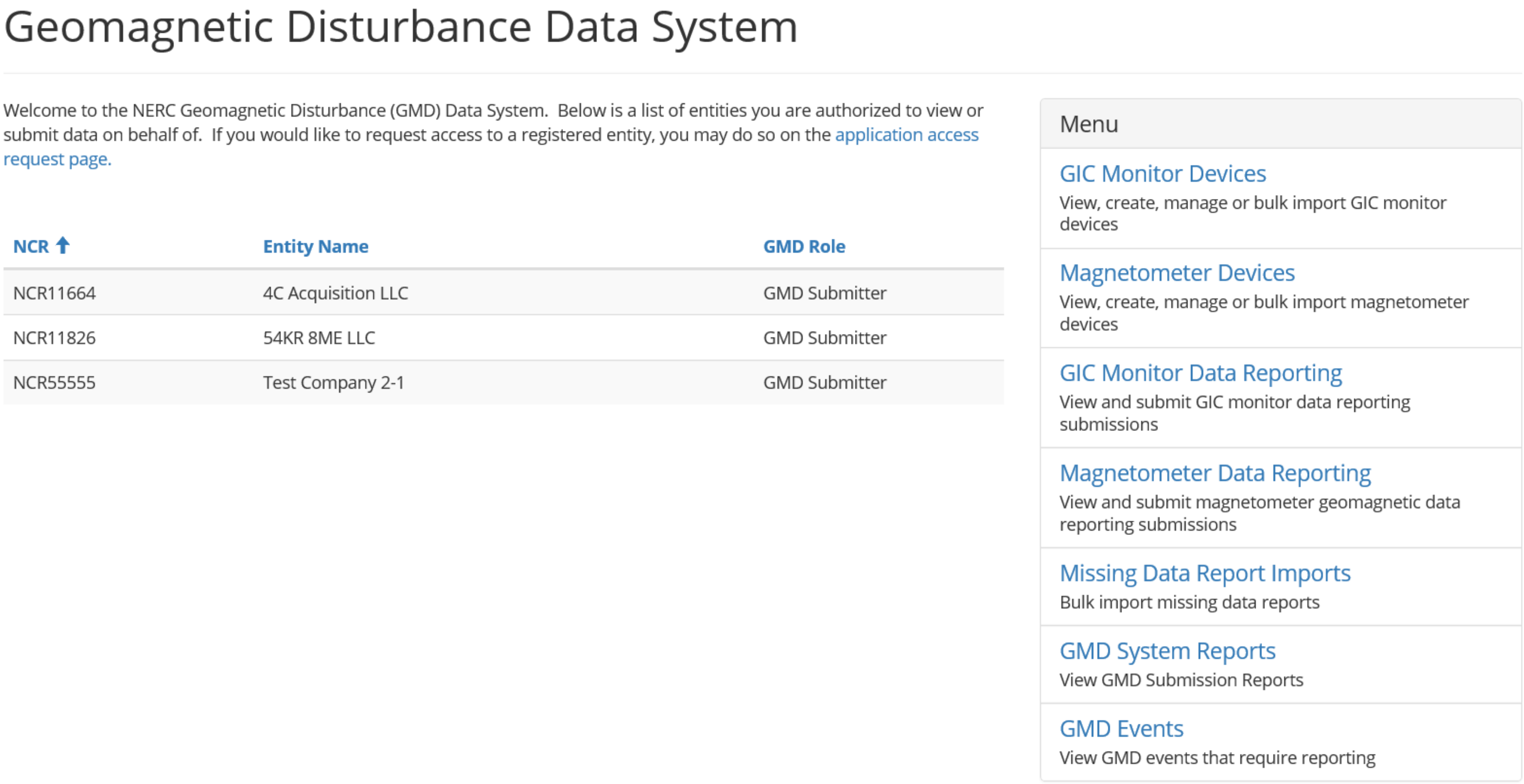
Geomagnetic Disturbance Data Reporting Instructions

Reporting Templates

Section 1600 Data Request

Proof of Concept

Submission Page and Main Menu



Geomagnetic Disturbance Data System

Welcome to the NERC Geomagnetic Disturbance (GMD) Data System. Below is a list of entities you are authorized to view or submit data on behalf of. If you would like to request access to a registered entity, you may do so on the application access request page.

NCR ↑	Entity Name	GMD Role
NCR11664	4C Acquisition LLC	GMD Submitter
NCR11826	54KR 8ME LLC	GMD Submitter
NCR55555	Test Company 2-1	GMD Submitter

Menu

GIC Monitor Devices
View, create, manage or bulk import GIC monitor devices

Magnetometer Devices
View, create, manage or bulk import magnetometer devices

GIC Monitor Data Reporting
View and submit GIC monitor data reporting submissions

Magnetometer Data Reporting
View and submit magnetometer geomagnetic data reporting submissions

Missing Data Report Imports
Bulk import missing data reports

GMD System Reports
View GMD Submission Reports

GMD Events
View GMD events that require reporting

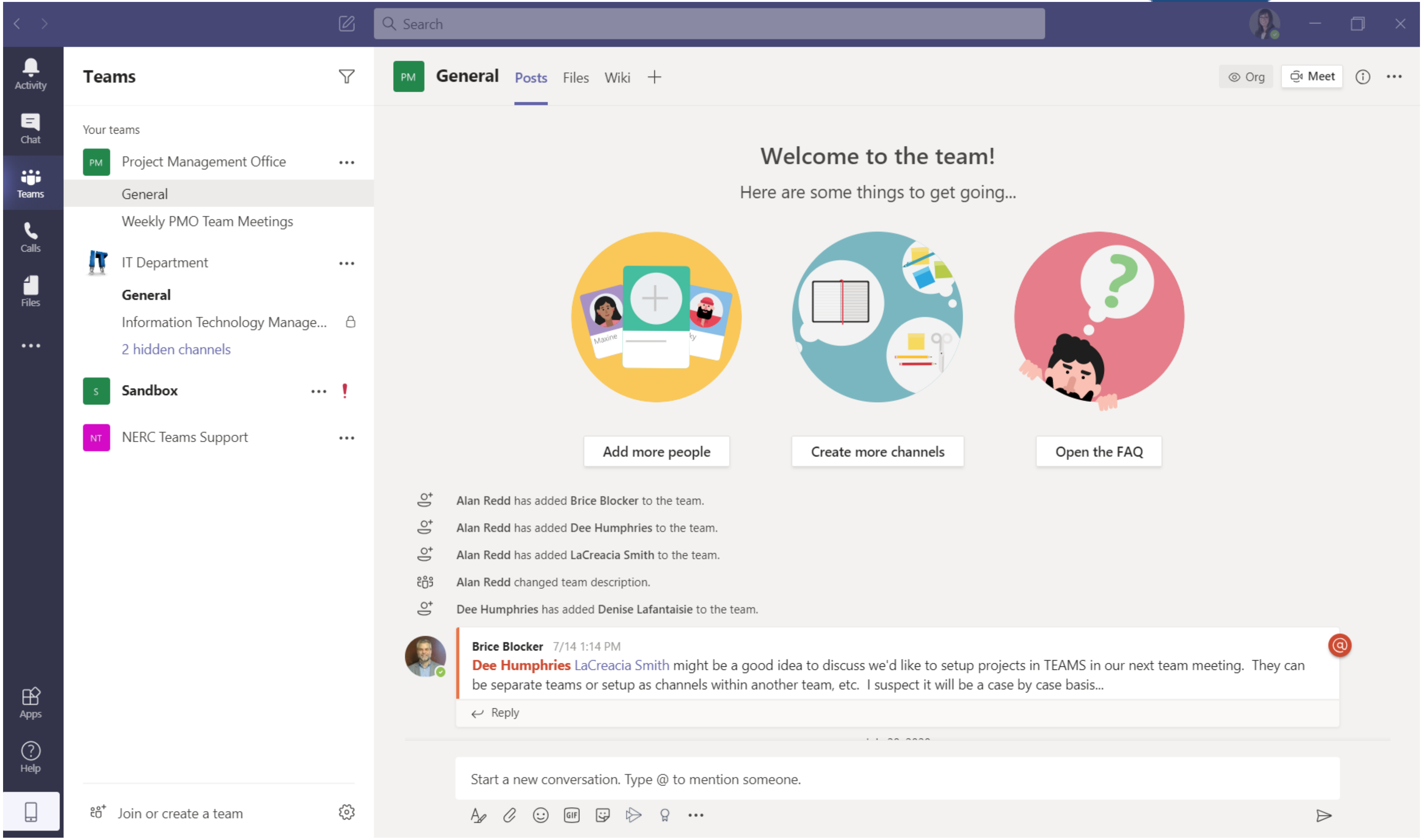
GMD Business Readiness

- Training
  - Regional registration teams will be encouraged to train entity users on Centralized Organization Registration ERO System changes
  - Two types of GMD training - one for reporting entities and the other for data researchers
  - Training and user documentation development – August 2020
  - Data reporting training sessions in – October 2020
  - Data Researcher training may be delayed until early 2021 to allow for a period of data collection in Q4 2020
- Inviting Electric Power Research Institute to participate as an entity submitter during user acceptance testing integration testing in September

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

Microsoft TEAMS



Welcome to the team!

Here are some things to get going...

Alan Redd has added Brice Blocker to the team.

Alan Redd has added Dee Humphries to the team.

Alan Redd has added LaCreacia Smith to the team.

Alan Redd changed team description.

Dee Humphries has added Denise Lafantaisie to the team.

Brice Blocker 7/14 1:14 PM

Dee Humphries LaCreacia Smith might be a good idea to discuss we'd like to setup projects in TEAMS in our next team meeting. They can be separate teams or setup as channels within another team, etc. I suspect it will be a case by case basis...

Start a new conversation. Type @ to mention someone.

E-ISAC

- CRM tool (Salesforce) in production, saving time and increasing accuracy of member tracking and stakeholder contacts
- E-ISAC Portal – Platform replacement to Salesforce underway; expected go live in Q4 2020
- E-ISAC Data Platform (EDP) – Converting to a robust, reliable, secure production platform in Atlanta data center; continue to expand analytical capabilities

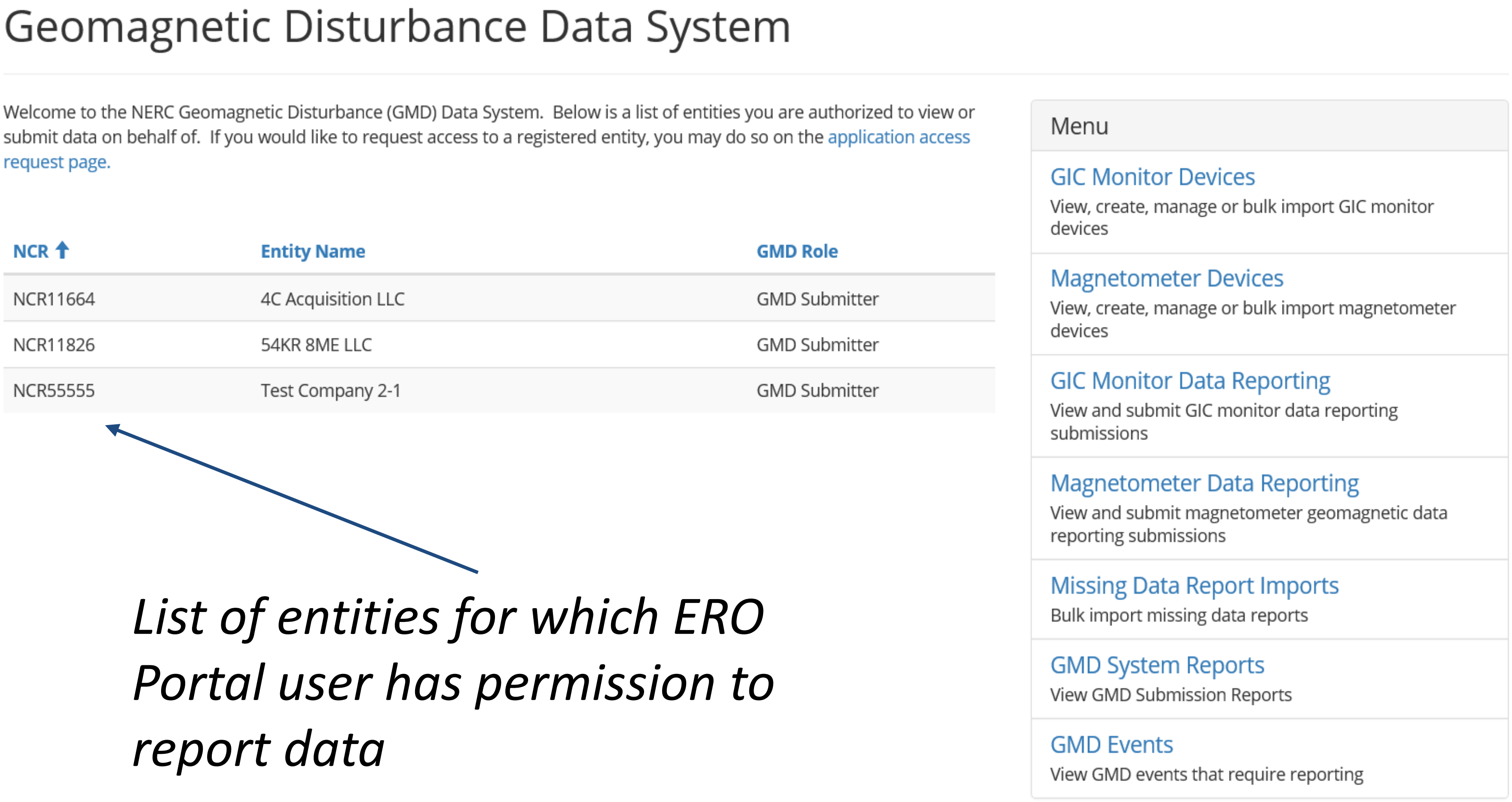
Priorities Looking Ahead

- Analytical capabilities for the E-ISAC under the EDP
- Accelerated adoption of Salesforce capabilities for the E-ISAC
- Implementation of Microsoft Teams
- Regional focus on cyber security with new cyber security director
- Various software/hardware upgrades to NERC infrastructure

Questions and Answers

GMD Application Screen Shots

Main Application Page for Data Submitters



Geomagnetic Disturbance Data System

Welcome to the NERC Geomagnetic Disturbance (GMD) Data System. Below is a list of entities you are authorized to view or submit data on behalf of. If you would like to request access to a registered entity, you may do so on the application access request page.

NCR ↑	Entity Name	GMD Role
NCR11664	4C Acquisition LLC	GMD Submitter
NCR11826	54KR 8ME LLC	GMD Submitter
NCR55555	Test Company 2-1	GMD Submitter

Menu

GIC Monitor Devices
View, create, manage or bulk import GIC monitor devices

Magnetometer Devices
View, create, manage or bulk import magnetometer devices

GIC Monitor Data Reporting
View and submit GIC monitor data reporting submissions

Magnetometer Data Reporting
View and submit magnetometer geomagnetic data reporting submissions

Missing Data Report Imports
Bulk import missing data reports

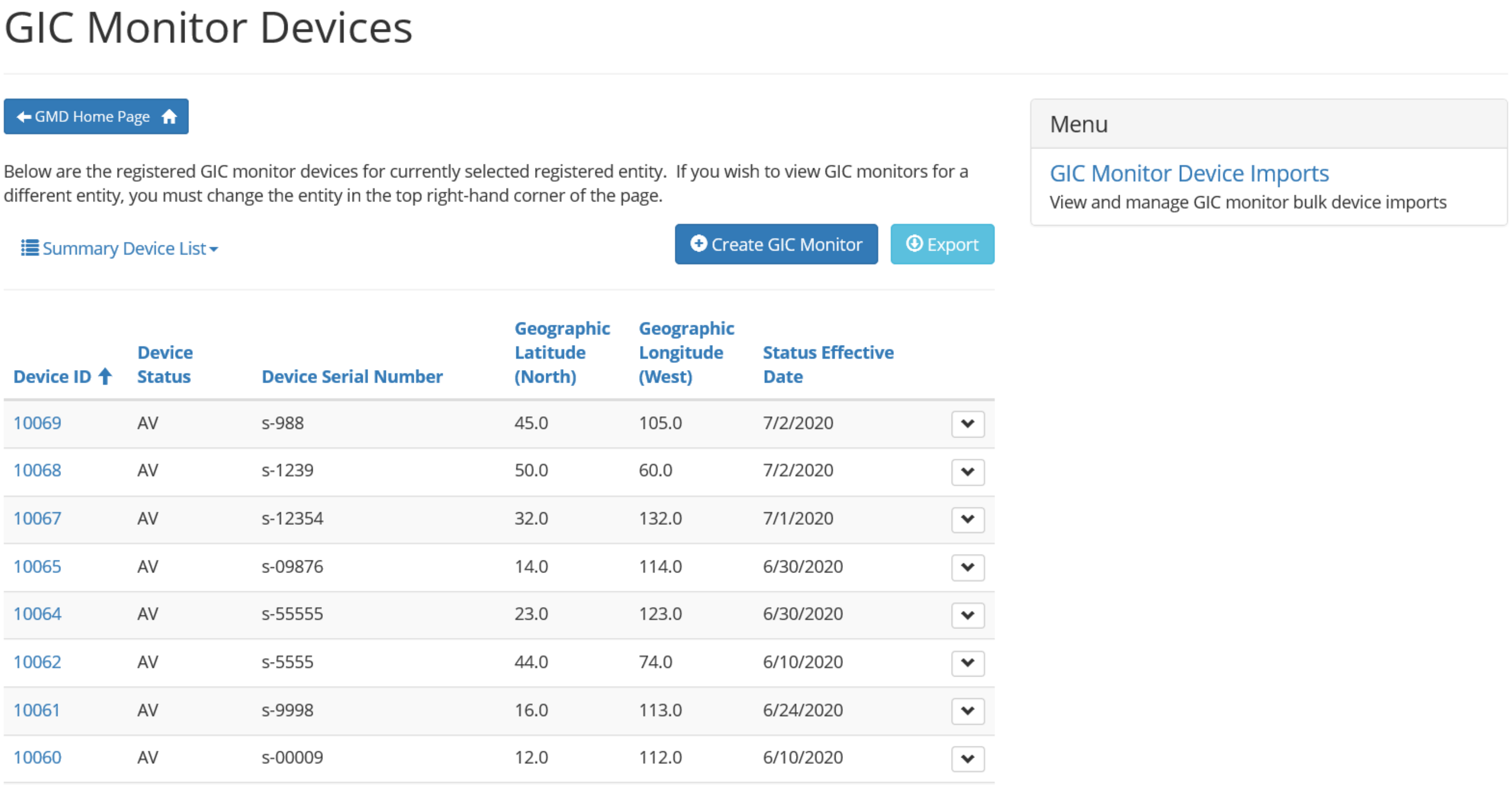
GMD System Reports
View GMD Submission Reports

GMD Events
View GMD events that require reporting

List of entities for which ERO Portal user has permission to report data

GIC Monitor Devices

- GIC Monitor Device Screen Displays Existing Devices and Provides Ability to Create or Edit, Manually or via Import File

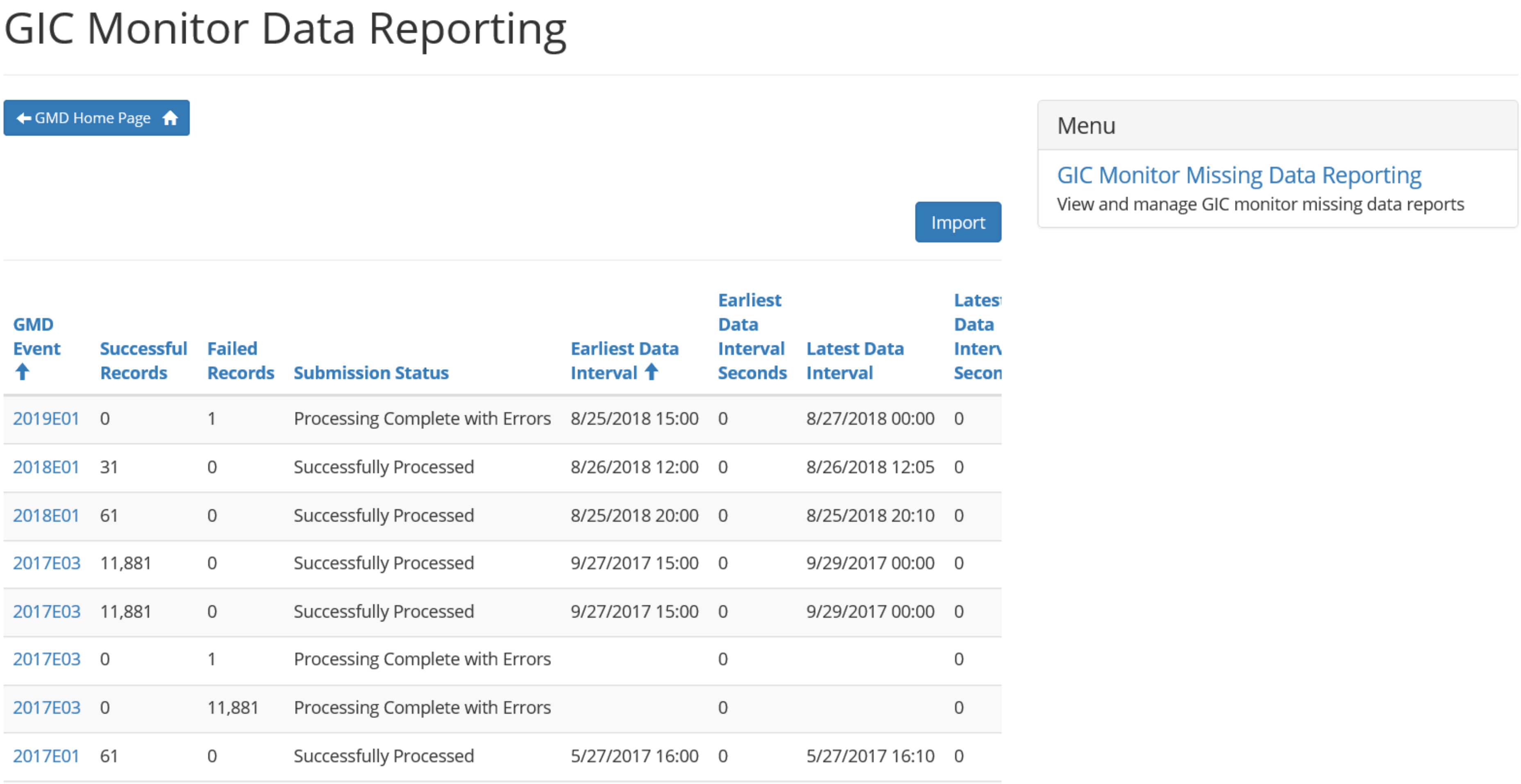


Below are the registered GIC monitor devices for currently selected registered entity. If you wish to view GIC monitors for a different entity, you must change the entity in the top right-hand corner of the page.

Device ID ↑	Device Status	Device Serial Number	Geographic Latitude (North)	Geographic Longitude (West)	Status Effective Date
10069	AV	s-988	45.0	105.0	7/2/2020
10068	AV	s-1239	50.0	60.0	7/2/2020
10067	AV	s-12354	32.0	132.0	7/1/2020
10065	AV	s-09876	14.0	114.0	6/30/2020
10064	AV	s-55555	23.0	123.0	6/30/2020
10062	AV	s-5555	44.0	74.0	6/10/2020
10061	AV	s-9998	16.0	113.0	6/24/2020
10060	AV	s-00009	12.0	112.0	6/10/2020

GIC Monitor Data Reporting

- GIC Monitor Device Import Validation Results



GIC Monitor Data Reporting

Menu

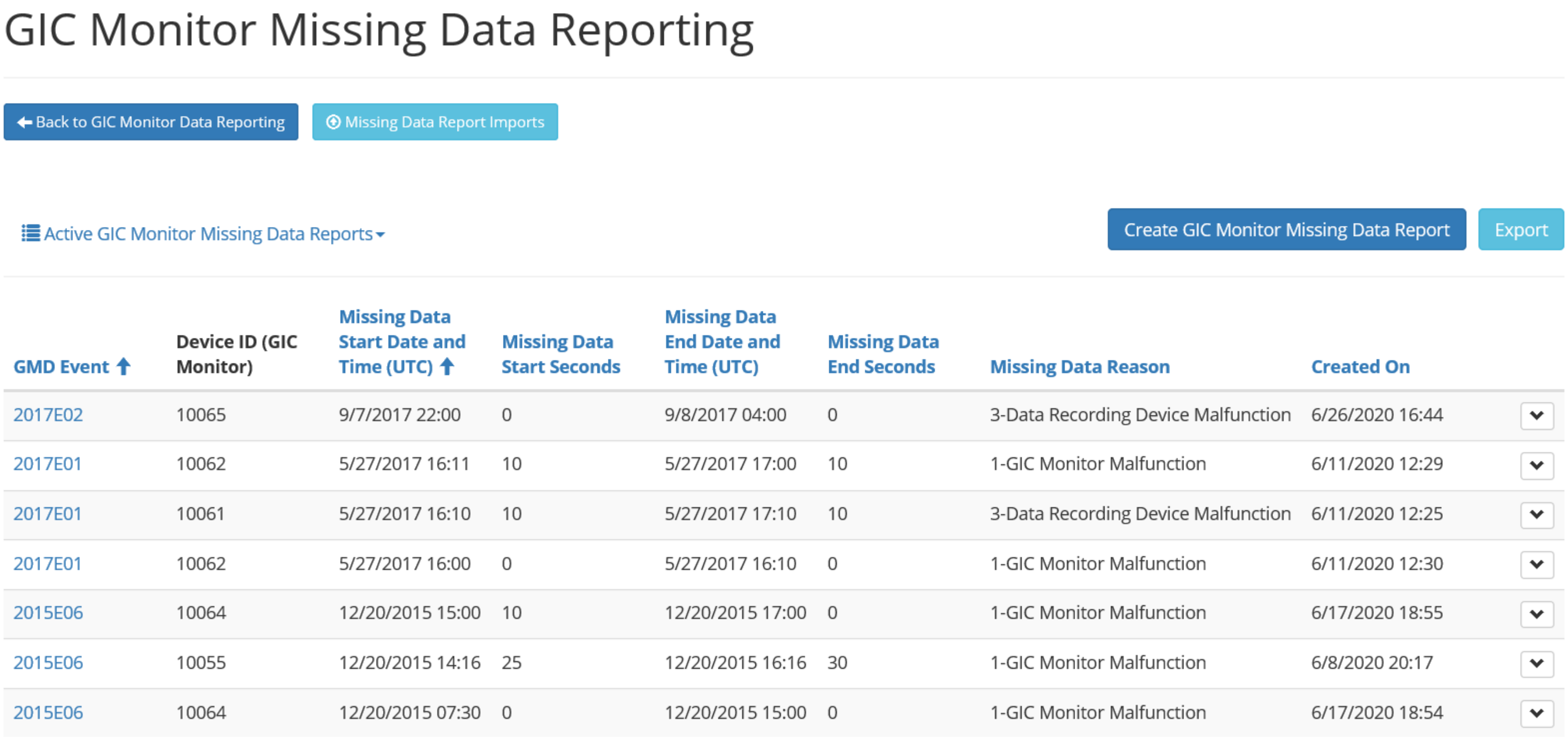
GIC Monitor Missing Data Reporting

View and manage GIC monitor missing data reports

GMD Event ↑	Successful Records	Failed Records	Submission Status	Earliest Data Interval ↑	Earliest Data Interval Seconds	Latest Data Interval	Lates Data Interv Secon
2019E01	0	1	Processing Complete with Errors	8/25/2018 15:00	0	8/27/2018 00:00	0
2018E01	31	0	Successfully Processed	8/26/2018 12:00	0	8/26/2018 12:05	0
2018E01	61	0	Successfully Processed	8/25/2018 20:00	0	8/25/2018 20:10	0
2017E03	11,881	0	Successfully Processed	9/27/2017 15:00	0	9/29/2017 00:00	0
2017E03	11,881	0	Successfully Processed	9/27/2017 15:00	0	9/29/2017 00:00	0
2017E03	0	1	Processing Complete with Errors		0		0
2017E03	0	11,881	Processing Complete with Errors		0		0
2017E01	61	0	Successfully Processed	5/27/2017 16:00	0	5/27/2017 16:10	0

GIC Monitor Missing Data Reporting

- Missing Data Reports Document Gaps in GMD Event Data



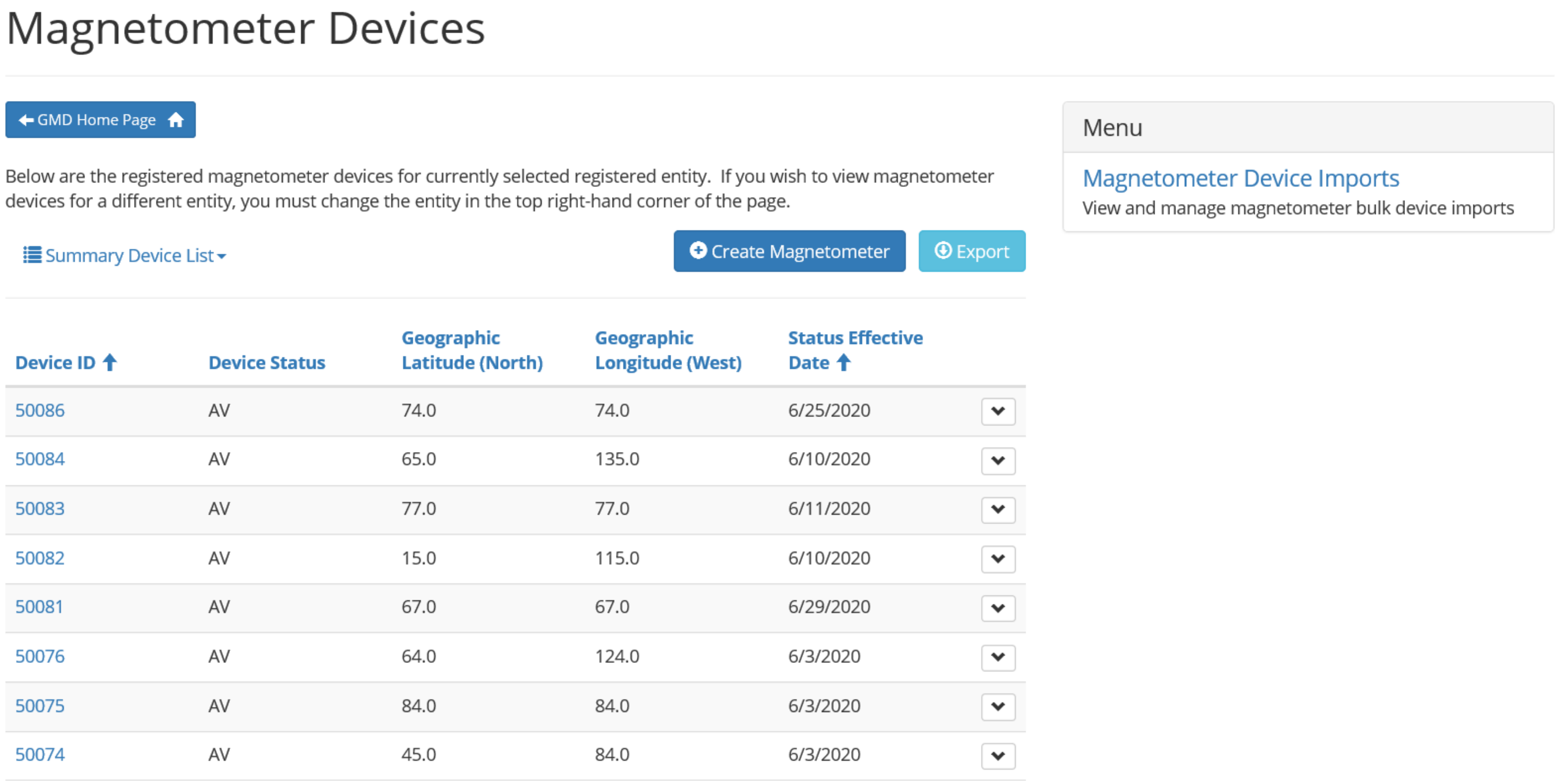
GIC Monitor Missing Data Reporting

← Back to GIC Monitor Data Reporting
Missing Data Report Imports
Active GIC Monitor Missing Data Reports ▾
Create GIC Monitor Missing Data Report
Export

GMD Event ↑	Device ID (GIC Monitor)	Missing Data Start Date and Time (UTC) ↑	Missing Data Start Seconds	Missing Data End Date and Time (UTC)	Missing Data End Seconds	Missing Data Reason	Created On	
2017E02	10065	9/7/2017 22:00	0	9/8/2017 04:00	0	3-Data Recording Device Malfunction	6/26/2020 16:44	⌄
2017E01	10062	5/27/2017 16:11	10	5/27/2017 17:00	10	1-GIC Monitor Malfunction	6/11/2020 12:29	⌄
2017E01	10061	5/27/2017 16:10	10	5/27/2017 17:10	10	3-Data Recording Device Malfunction	6/11/2020 12:25	⌄
2017E01	10062	5/27/2017 16:00	0	5/27/2017 16:10	0	1-GIC Monitor Malfunction	6/11/2020 12:30	⌄
2015E06	10064	12/20/2015 15:00	10	12/20/2015 17:00	0	1-GIC Monitor Malfunction	6/17/2020 18:55	⌄
2015E06	10055	12/20/2015 14:16	25	12/20/2015 16:16	30	1-GIC Monitor Malfunction	6/8/2020 20:17	⌄
2015E06	10064	12/20/2015 07:30	0	12/20/2015 15:00	0	1-GIC Monitor Malfunction	6/17/2020 18:54	⌄

Magnetometer Devices

- Magnetometer Device Screen Displays Existing Devices and Provides Ability to Create or Edit, Manually or via Import File



Magnetometer Devices

Below are the registered magnetometer devices for currently selected registered entity. If you wish to view magnetometer devices for a different entity, you must change the entity in the top right-hand corner of the page.

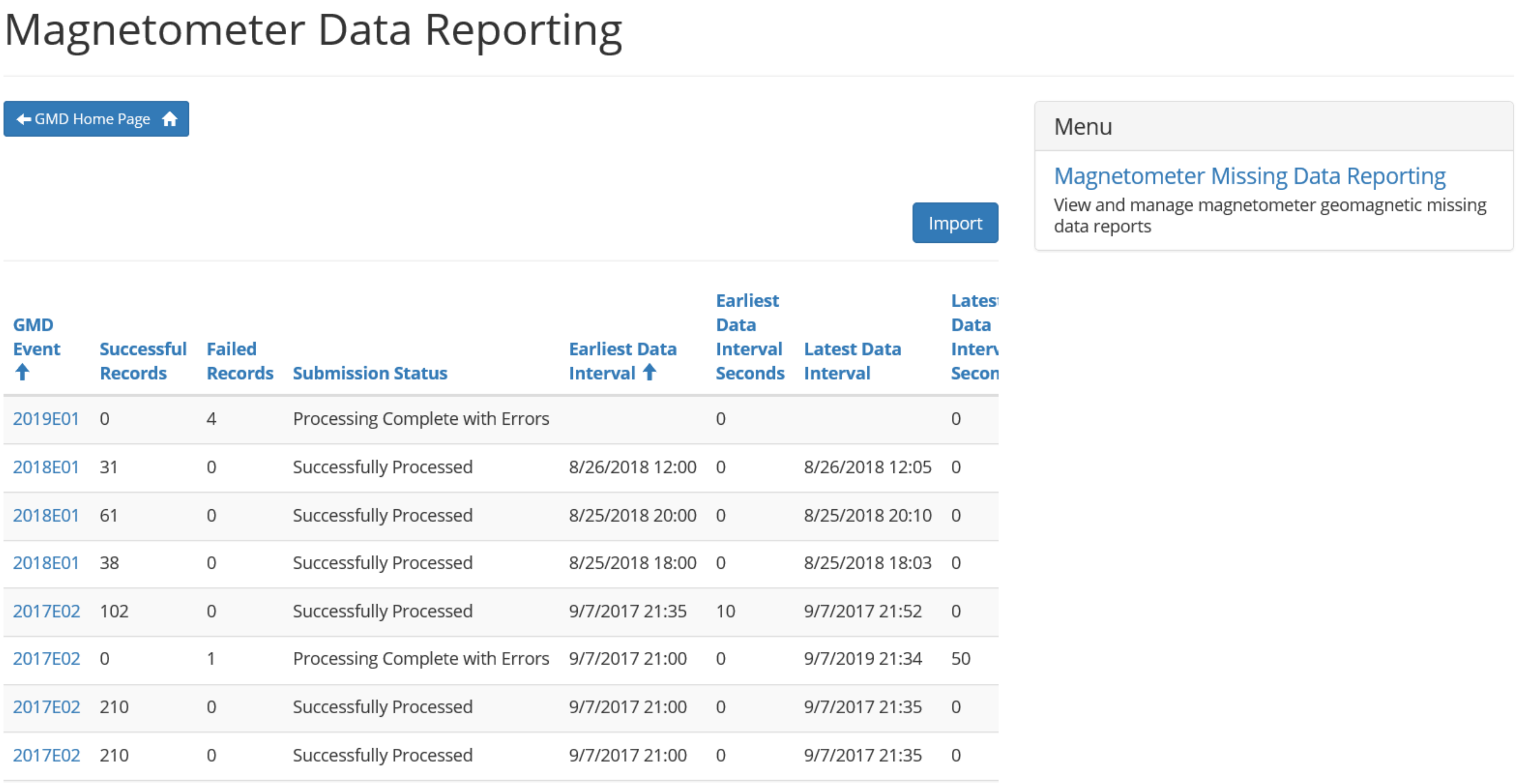
Device ID ↑	Device Status	Geographic Latitude (North)	Geographic Longitude (West)	Status Effective Date ↑
50086	AV	74.0	74.0	6/25/2020
50084	AV	65.0	135.0	6/10/2020
50083	AV	77.0	77.0	6/11/2020
50082	AV	15.0	115.0	6/10/2020
50081	AV	67.0	67.0	6/29/2020
50076	AV	64.0	124.0	6/3/2020
50075	AV	84.0	84.0	6/3/2020
50074	AV	45.0	84.0	6/3/2020

Magnetometer Device Imports

View and manage magnetometer bulk device imports

Magnetometer Data Reporting

- Magnetometer Device Import Validation Results



Magnetometer Data Reporting

GMD Event ↑	Successful Records	Failed Records	Submission Status	Earliest Data Interval ↑	Earliest Data Interval Seconds	Latest Data Interval	Lates Data Interv Secon
2019E01	0	4	Processing Complete with Errors		0		0
2018E01	31	0	Successfully Processed	8/26/2018 12:00	0	8/26/2018 12:05	0
2018E01	61	0	Successfully Processed	8/25/2018 20:00	0	8/25/2018 20:10	0
2018E01	38	0	Successfully Processed	8/25/2018 18:00	0	8/25/2018 18:03	0
2017E02	102	0	Successfully Processed	9/7/2017 21:35	10	9/7/2017 21:52	0
2017E02	0	1	Processing Complete with Errors	9/7/2017 21:00	0	9/7/2019 21:34	50
2017E02	210	0	Successfully Processed	9/7/2017 21:00	0	9/7/2017 21:35	0
2017E02	210	0	Successfully Processed	9/7/2017 21:00	0	9/7/2017 21:35	0

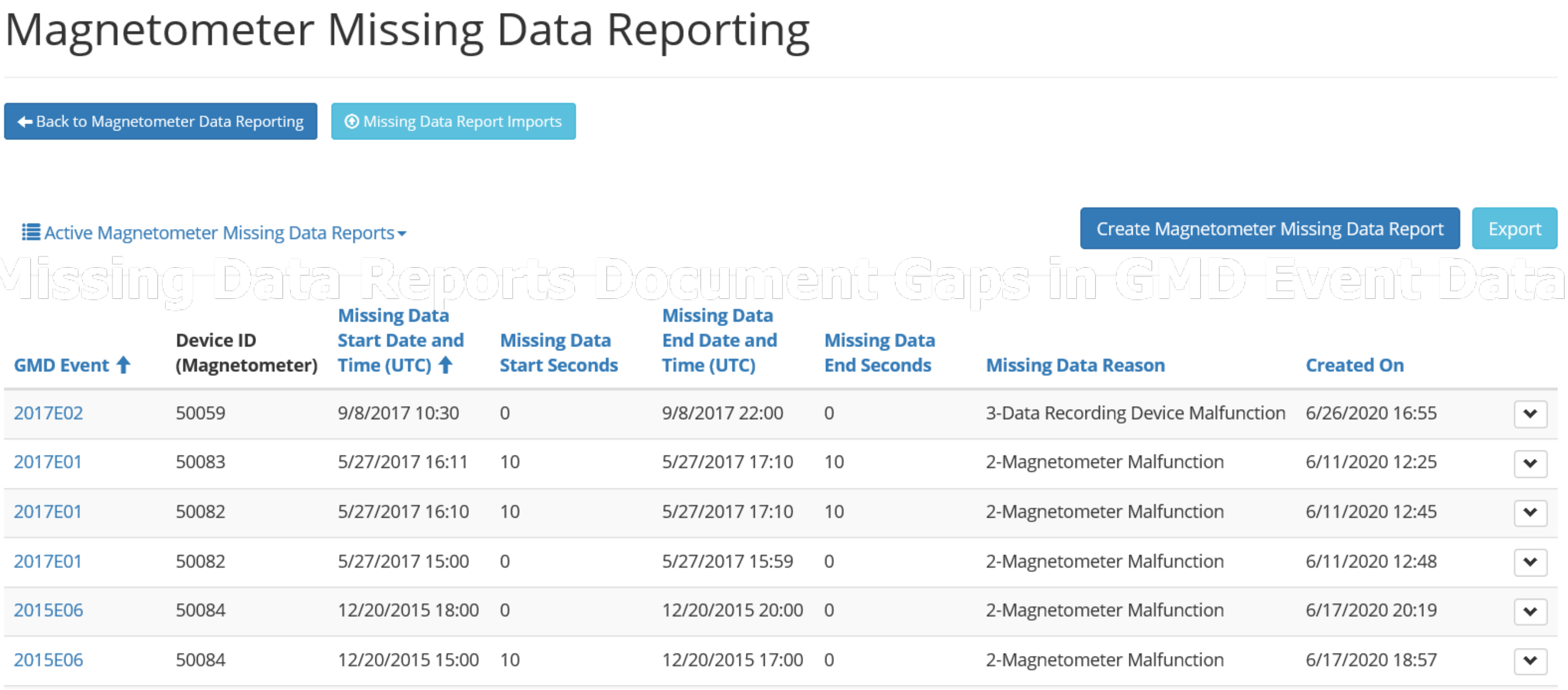
Menu

Magnetometer Missing Data Reporting

View and manage magnetometer geomagnetic missing data reports

Magnetometer Missing Data Reporting

- Missing Data Reports Document Gaps in GMD Event Data



Magnetometer Missing Data Reporting

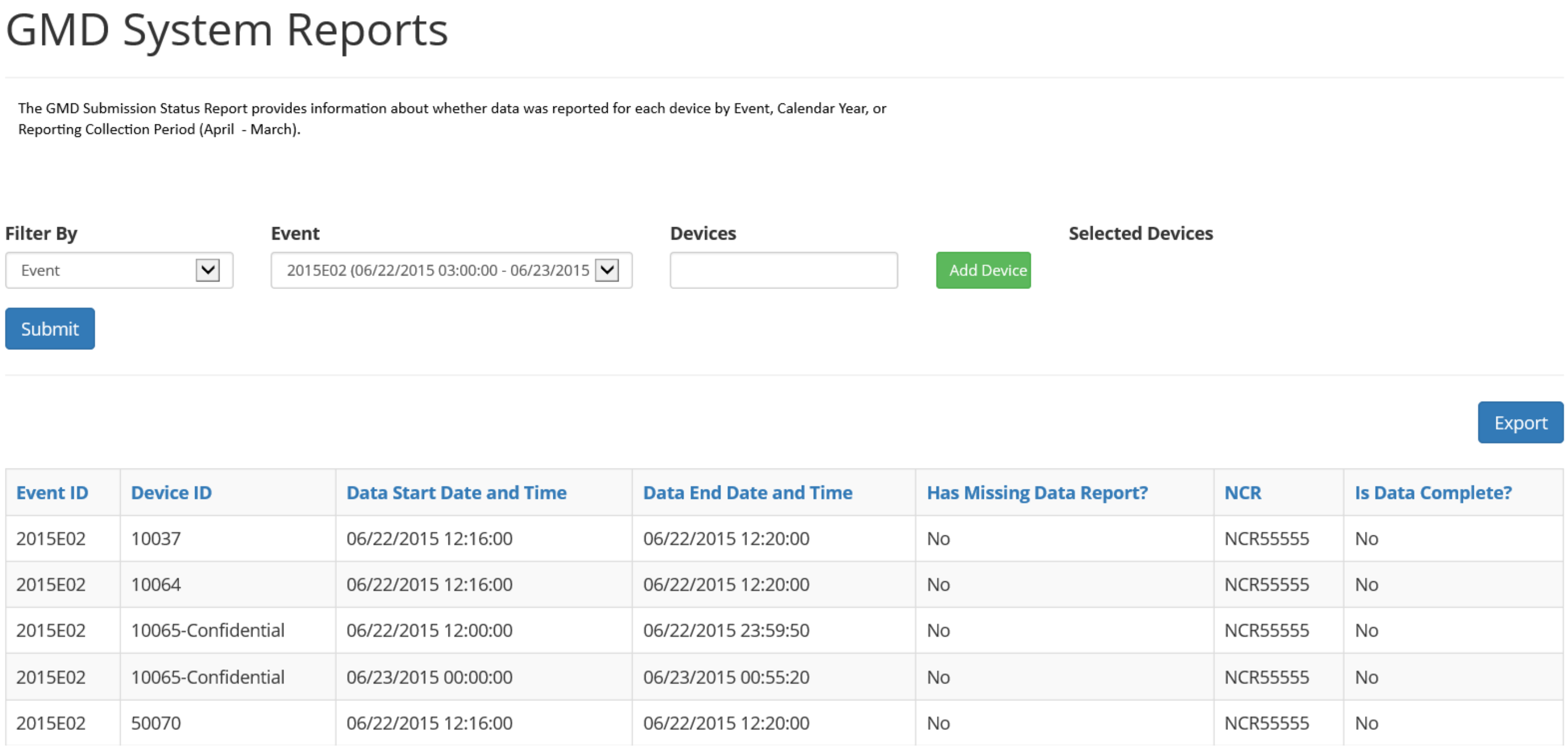
← Back to Magnetometer Data Reporting
Missing Data Report Imports
Active Magnetometer Missing Data Reports ▾
Create Magnetometer Missing Data Report
Export

Missing Data Reports Document Gaps in GMD Event Data

GMD Event ↑	Device ID (Magnetometer)	Missing Data Start Date and Time (UTC) ↑	Missing Data Start Seconds	Missing Data End Date and Time (UTC)	Missing Data End Seconds	Missing Data Reason	Created On	
2017E02	50059	9/8/2017 10:30	0	9/8/2017 22:00	0	3-Data Recording Device Malfunction	6/26/2020 16:55	⌄
2017E01	50083	5/27/2017 16:11	10	5/27/2017 17:10	10	2-Magnetometer Malfunction	6/11/2020 12:25	⌄
2017E01	50082	5/27/2017 16:10	10	5/27/2017 17:10	10	2-Magnetometer Malfunction	6/11/2020 12:45	⌄
2017E01	50082	5/27/2017 15:00	0	5/27/2017 15:59	0	2-Magnetometer Malfunction	6/11/2020 12:48	⌄
2015E06	50084	12/20/2015 18:00	0	12/20/2015 20:00	0	2-Magnetometer Malfunction	6/17/2020 20:19	⌄
2015E06	50084	12/20/2015 15:00	10	12/20/2015 17:00	0	2-Magnetometer Malfunction	6/17/2020 18:57	⌄

GMD System Reports

- Submission Status Report Shows Device Reporting for an Event



GMD System Reports

The GMD Submission Status Report provides information about whether data was reported for each device by Event, Calendar Year, or Reporting Collection Period (April - March).

Filter By: Event

Event: 2015E02 (06/22/2015 03:00:00 - 06/23/2015

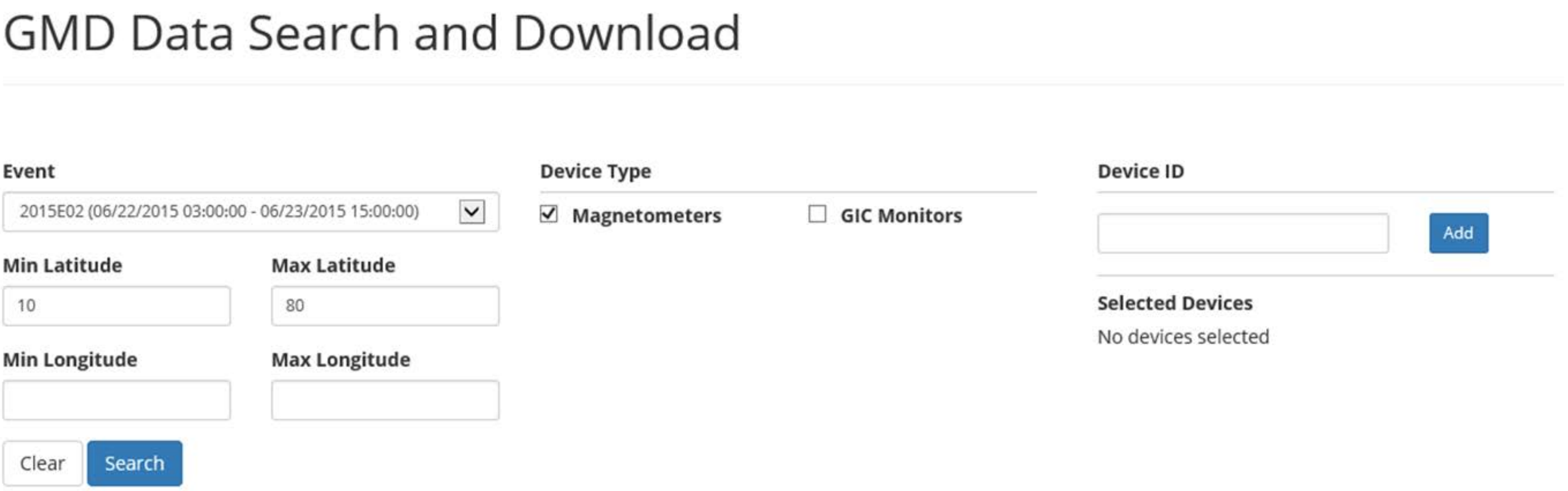
Devices:

Selected Devices:

Event ID	Device ID	Data Start Date and Time	Data End Date and Time	Has Missing Data Report?	NCR	Is Data Complete?
2015E02	10037	06/22/2015 12:16:00	06/22/2015 12:20:00	No	NCR55555	No
2015E02	10064	06/22/2015 12:16:00	06/22/2015 12:20:00	No	NCR55555	No
2015E02	10065-Confidential	06/22/2015 12:00:00	06/22/2015 23:59:50	No	NCR55555	No
2015E02	10065-Confidential	06/23/2015 00:00:00	06/23/2015 00:55:20	No	NCR55555	No
2015E02	50070	06/22/2015 12:16:00	06/22/2015 12:20:00	No	NCR55555	No

GMD Data Search and Download

- Data Search and Download Allows Researchers to Specify Criteria



GMD Data Search and Download

Event: 2015E02 (06/22/2015 03:00:00 - 06/23/2015 15:00:00)

Min Latitude: 10

Max Latitude: 80

Min Longitude:

Max Longitude:

Device Type: ☑ Magnetometers □ GIC Monitors

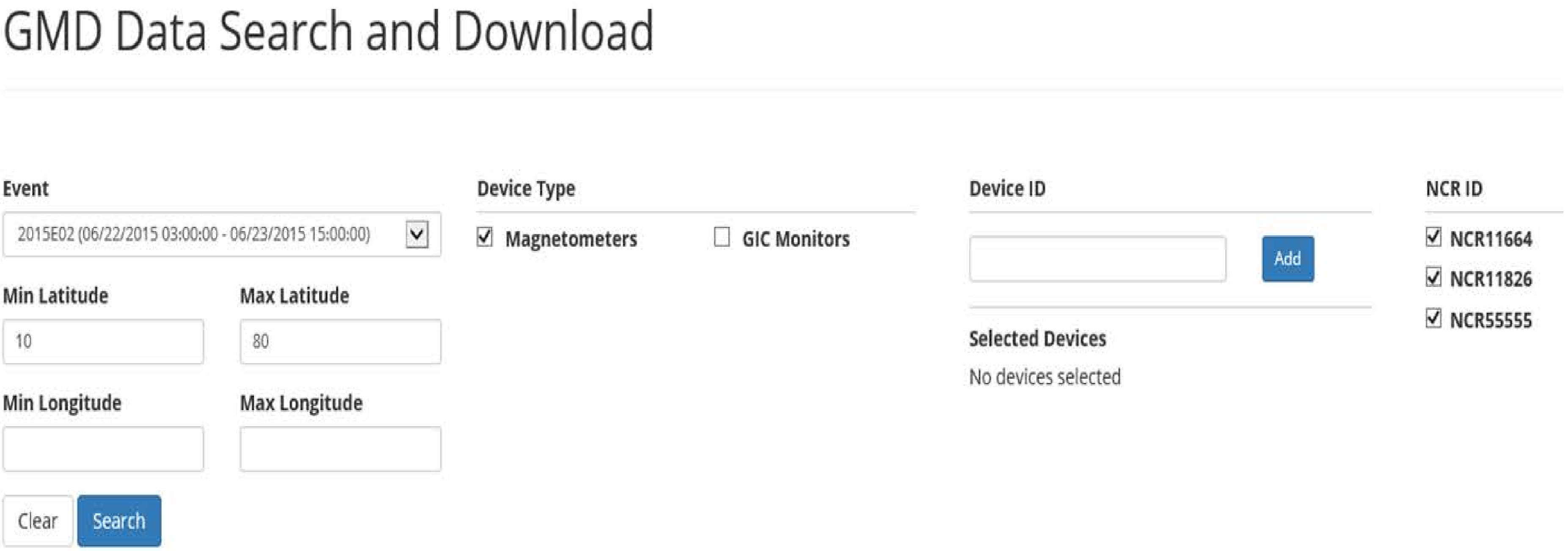
Device ID:

Selected Devices

No devices selected

GMD Data Search and Download

- GMD Data Submitters Also Can Search by Entity NCR ID



GMD Data Search and Download

Event

2015E02 (06/22/2015 03:00:00 - 06/23/2015 15:00:00)

Min Latitude: 10

Max Latitude: 80

Min Longitude:

Max Longitude:

Device Type

☑ Magnetometers

☐ GIC Monitors

Device ID

Selected Devices

No devices selected

NCR ID

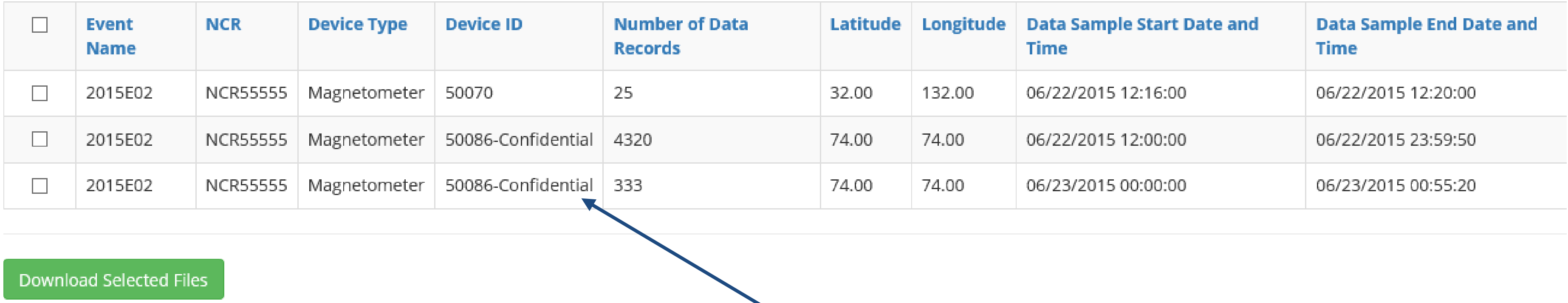
☑ NCR11664

☑ NCR11826

☑ NCR55555

GMD Data Search and Download

- Data Search and Download Results Displayed; User Selects Data Files to Download



□	Event Name	NCR	Device Type	Device ID	Number of Data Records	Latitude	Longitude	Data Sample Start Date and Time	Data Sample End Date and Time
□	2015E02	NCR55555	Magnetometer	50070	25	32.00	132.00	06/22/2015 12:16:00	06/22/2015 12:20:00
□	2015E02	NCR55555	Magnetometer	50086-Confidential	4320	74.00	74.00	06/22/2015 12:00:00	06/22/2015 23:59:50
□	2015E02	NCR55555	Magnetometer	50086-Confidential	333	74.00	74.00	06/23/2015 00:00:00	06/23/2015 00:55:20

Confidential data files only provided to entities who report those devices

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise Align Project Update

Stan Hoptroff, Vice President, Business Technology

Technology and Security Committee Meeting

August 19, 2020

RELIABILITY | RESILIENCE | SECURITY

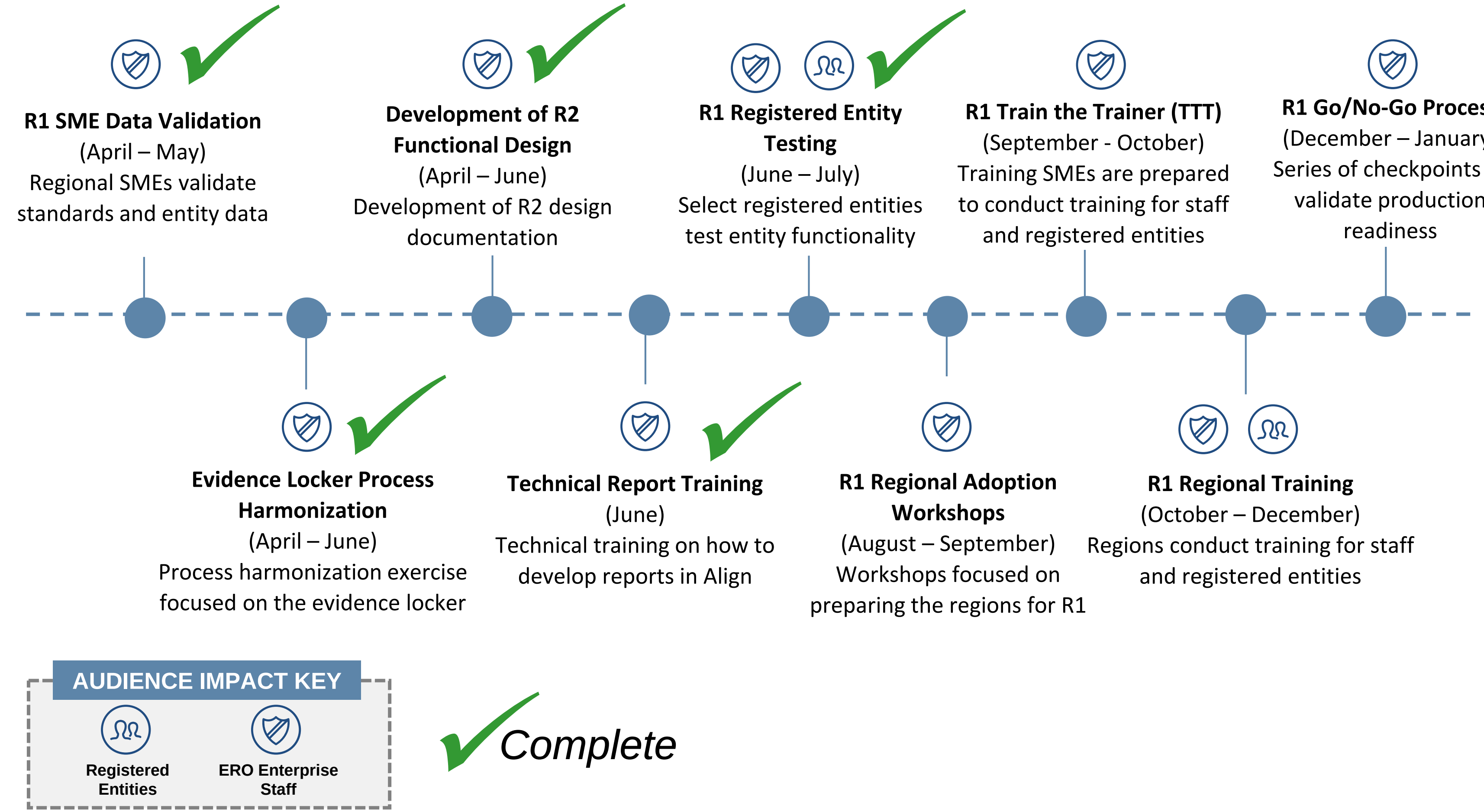
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Agenda

- Major/New Topics
    - Release 1 Timeline Overview
    - Registered Entity Testing Schedule and Participants
    - Registered Entity Feedback
    - Align Governance Model
    - Canada
    - Challenges
    - How to Stay Informed
    - Upcoming Milestones
    - What to Expect
    - Benefits

Release 1 Timeline Overview

The following is a timeline of upcoming key activities:



R1 SME Data Validation ✓
(April – May)
Regional SMEs validate standards and entity data

Evidence Locker Process Harmonization ✓
(April – June)
Process harmonization exercise focused on the evidence locker

Development of R2 Functional Design ✓
(April – June)
Development of R2 design documentation

Technical Report Training ✓
(June)
Technical training on how to develop reports in Align

R1 Registered Entity Testing ✓
(June – July)
Select registered entities test entity functionality

R1 Regional Adoption Workshops
(August – September)
Workshops focused on preparing the regions for R1

R1 Train the Trainer (TTT)
(September - October)
Training SMEs are prepared to conduct training for staff and registered entities

R1 Regional Training
(October – December)
Regions conduct training for staff and registered entities

R1 Go/No-Go Process
(December – January)
Series of checkpoints to validate production readiness

AUDIENCE IMPACT KEY

Registered Entities

ERO Enterprise Staff

✓ *Complete*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Entity Testing Schedule and Participants

Session	Date & Time
Kickoff and Logistics	June 18 (1 – 2 PM ET)
MRO Testing	July 7 (1 – 4:30 PM ET)
WECC Testing	July 8 (10:30 – 2 PM ET)
TRE Testing	July 13 (2 – 5:30 PM ET)
NPCC Testing	July 14 (8:30 – 12 PM ET)
RF Testing	July 15 (1 – 4:30 PM ET)
SERC Testing	July 22 (1 – 4:30 PM ET)

Tester/Representative	Company	Region
Jennifer Flandermeyer	Evergy	MRO
Tiffany Lake	Evergy	MRO
Mandy Barta	Evergy	MRO
Omar Elabbady	Xcel Energy	MRO
Thad Ness	Xcel Energy	MRO
Ashley Stringer	Oklahoma Municipal Power Authority	MRO
Tammy Porter	Oncor	TRE
Martha Henson	Oncor	TRE
Lee Maurer	Oncor	TRE
Amelia Anderson	CenterPoint	TRE
Daniela Hammons	CenterPoint	TRE
Venona Greaff	OXY	TRE
Kimberly Tolbert	OXY	TRE
Betty Day	ERCOT	TRE
Christine Hasha	ERCOT	TRE
Collen Frosch	ERCOT	TRE
Lisa Milanes	CAISO	WECC
Marty Hostler	NCPA	WECC
Scott Tomashefsky	NCPA	WECC
Catalina Hansen	SoCalEdison	WECC
HeCareth Wosu	SoCalEdison	WECC
John Pespisa	*SoCalEdison*	*WECC*
Kelley Stevens	SoCalEdison	WECC
Matt Goldberg	ISO-NE	NPCC
Greg Campoli	NYISO	NPCC
Patti Metro	NRECA	SERC?
Mark Pratt	Southern Co	SERC
Brandon Cain	Southern Co	SERC
Marsha Morgan	Southern Co	SERC
Roy O’Neal Kiser Jr	Southern Co	SERC
Silvia Parada Mitchell	FPL	SERC
Carol Chinn / Truong Le (covering for Carol)	FMPA	SERC
Jennifer Sterling	Exelon	RF
Kinte Whitehead	Exelon	RF
Rajesh Varghese	Exelon	RF
Rachel Snead	Dominion	RF

Registered Entity Feedback

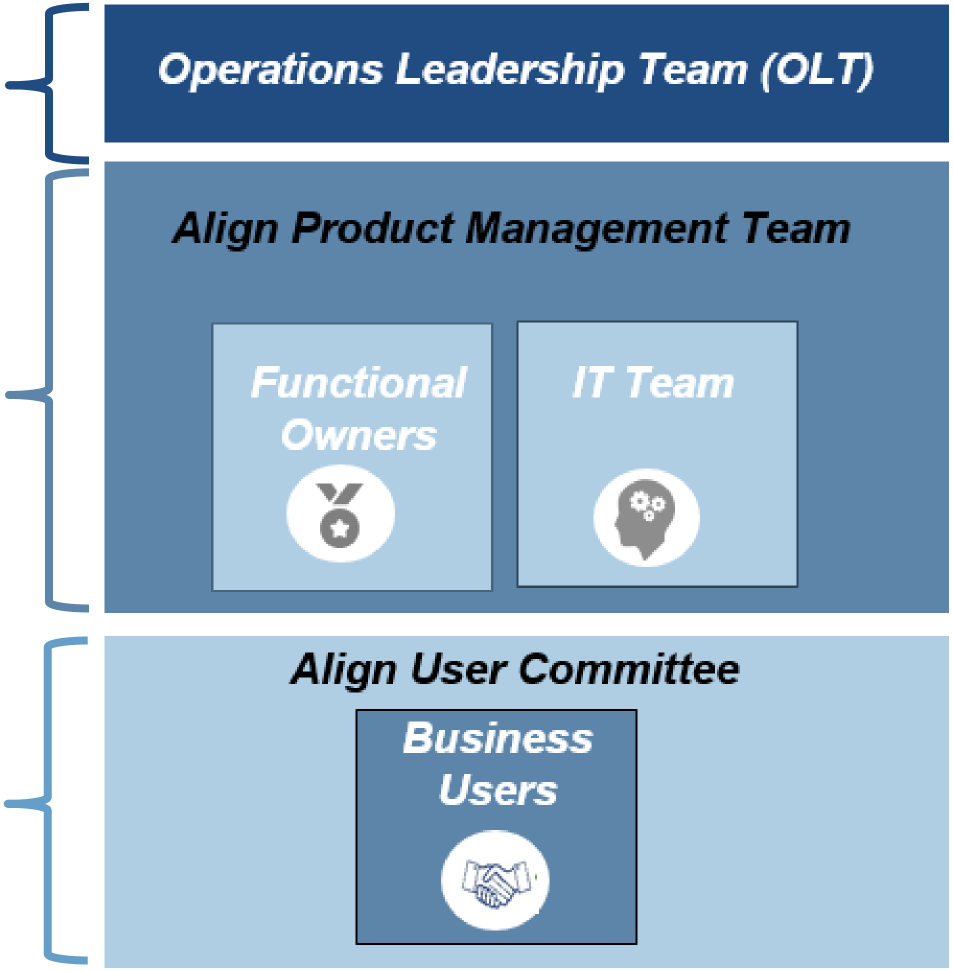
- What was tested
  - Self-report, mitigation and enforcement workflows and business rules
  - Dashboards and notifications
- Overall feedback
  - Positive feedback on the Regions' preparation and testing experience
  - Acknowledged the progress from earlier demos of Align
  - Complementary of the training materials
  - Requested a similar opportunity to test the ERO Enterprise Secure Evidence Locker (ERO SEL) when ready
  - Requested more engagement around Standards reporting
  - Some expressed disappointment that there are still two systems (Align and ERO SEL) but understand the business case
  - Approximately 50 enhancement requests were logged for consideration

Align Governance

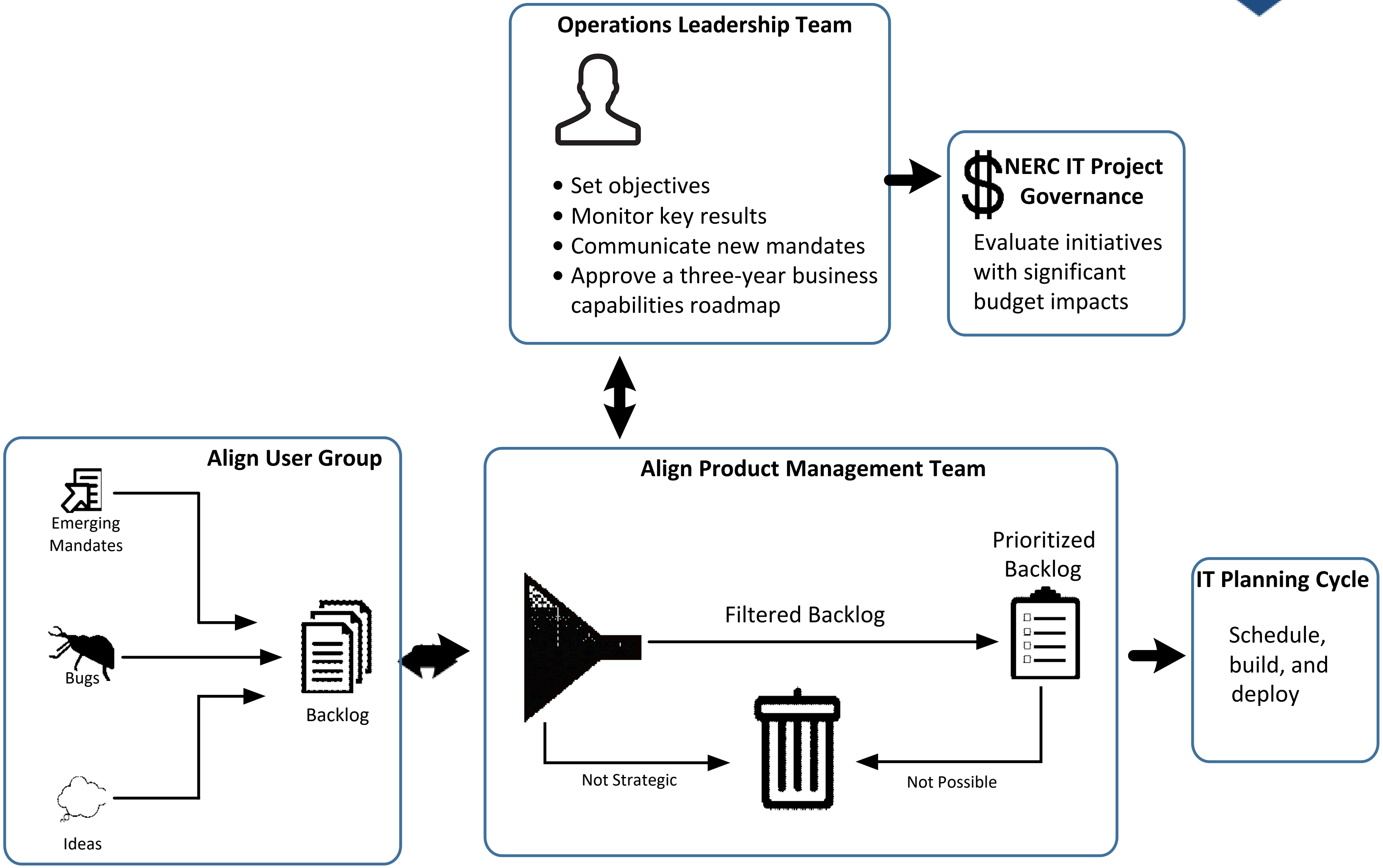
OLT: Provide executive leadership and oversight

Product Management Team: Risk Performance and Monitoring Group, Enforcement Group and NERC representation; project-level engagement

User Committee: Regional experts and registered entity experts representation; Compliance and Certification Committee and Alignment Working Group provides input and expertise


Operations Leadership Team (OLT)
Align Product Management Team
Functional Owners
IT Team
Align User Committee
Business Users

Align Governance



Operations Leadership Team

- Set objectives
- Monitor key results
- Communicate new mandates
- Approve a three-year business capabilities roadmap

NERC IT Project Governance

Evaluate initiatives with significant budget impacts

Align User Group

Align Product Management Team

IT Planning Cycle

Schedule, build, and deploy

Canada

- Determine which provinces will use the U.S. BWise instance
- Define use cases by Region and province
- Identify roadblocks (agreements, data sovereignty, etc.)
- Define rollout strategy for each province

Challenges

- **Resources:** multiple parallel efforts (R1 training/rollout, R2 development, R3 requirements, ongoing stakeholder engagement)
- **Budget pressure:** balance in-scope efforts with continuous improvement requests (i.e., 50 enhancements from stakeholders)
- **Rollout approach:** data supports “whole Region” vs. segmentation by groups of entities; management across multiple systems during rollout

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 Compliance Monitoring and Enforcement Program (CMEP) Regional workshops
- Trades meetings

Upcoming Milestones

Milestone	Completion Date
Training Materials (Videos, User Guides, Reference Materials)	September 2020
Regional Adoption Workshops	October 2020
Train Regional Training Leads	October/November 2020
Begin Regional Staff Training	November 2020
Change Agent Preparations	Ongoing

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, Periodic Data Submittals (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 Future Releases: What to expect?

Release 2 Functionality Est. 2021

- Technical Feasibility Exceptions
- Self-Certifications
- PDSs

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

Align - Benefits

Moving to a common platform will provide:

- Alignment of **common** & 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

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Secure Evidence Locker Update

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
August 19, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

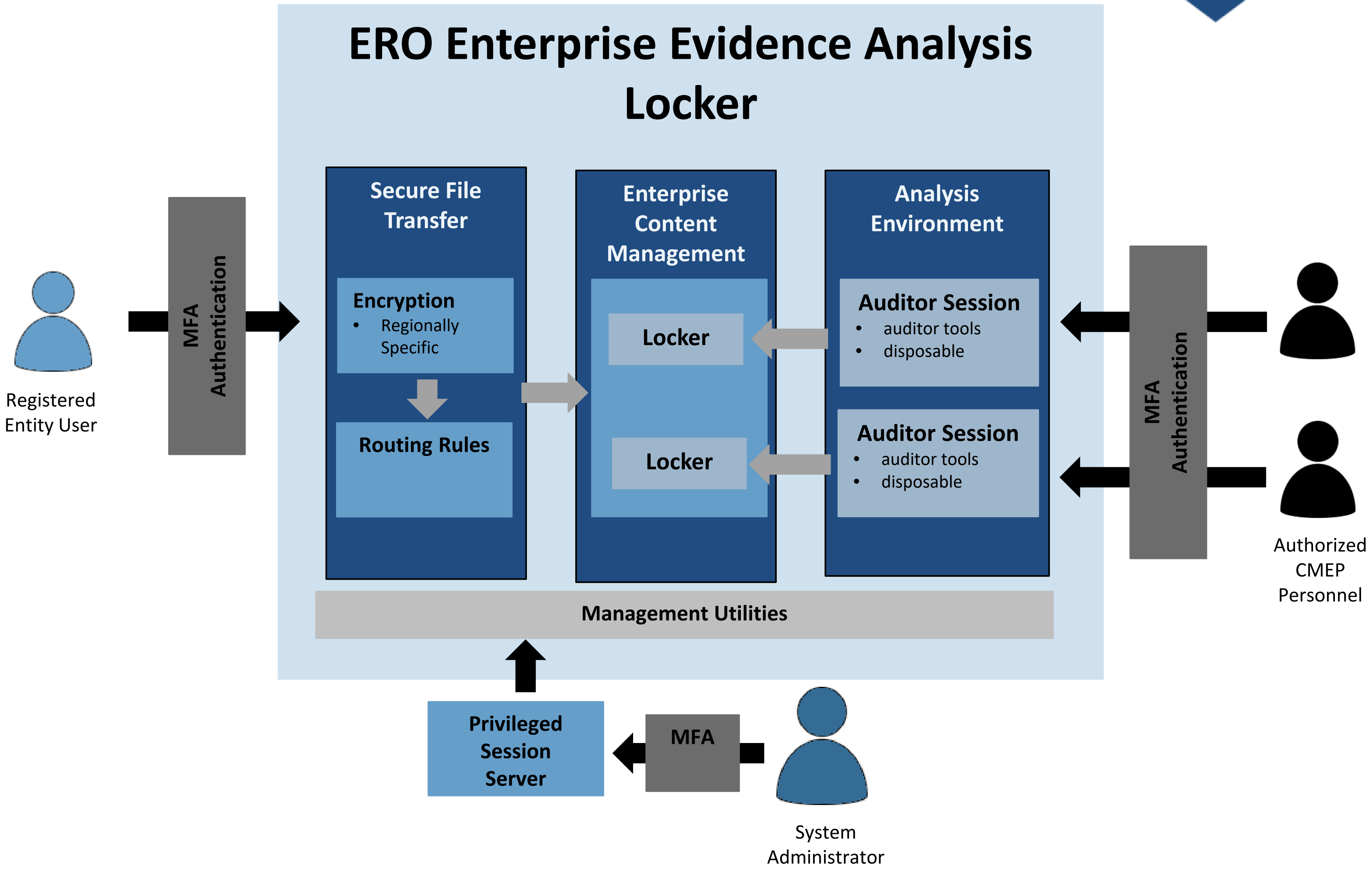
- What is the ERO Enterprise Secure Evidence Locker (ERO SEL)?
- Solution Overview
  - ERO SEL - How Will It Work?
  - National Institute of Standards and Technology (NIST) Standard
- Registered Entity Experience Screen Shots
- Regional Entity Experience Screen Shots
- ERO SEL Potential Risks

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

Solution Overview

ERO SEL - How will it work? Technical Implementation



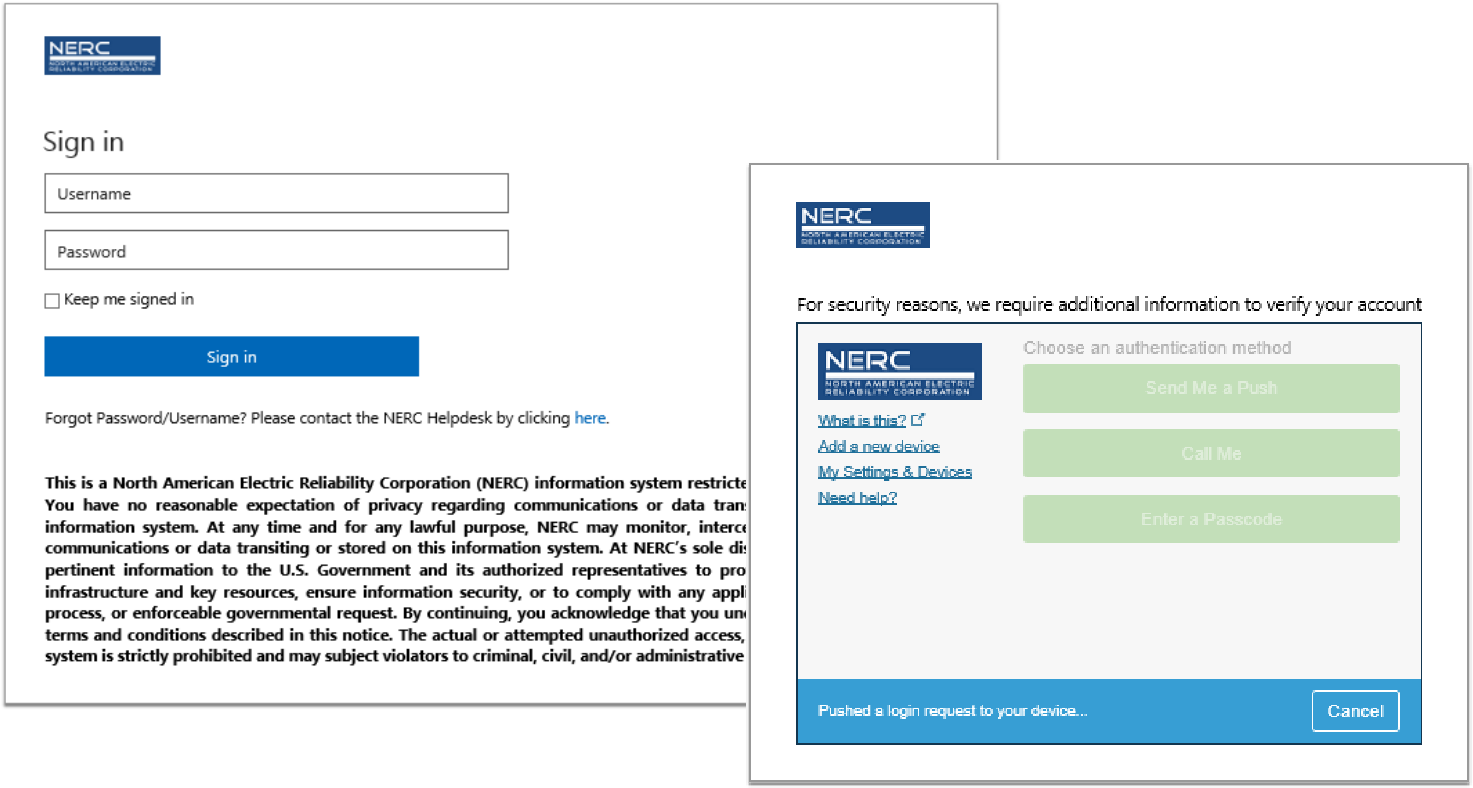
NIST Standard

- 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

Registered Entity Experience

ERO SEL – Registered Entity Experience

- Users will log into the Secure Evidence Locker through a URL and be authenticated using their ERO Portal account with Multi-Factor Authentication (MFA)



Forgot Password/Username? Please contact the NERC Helpdesk by clicking here.

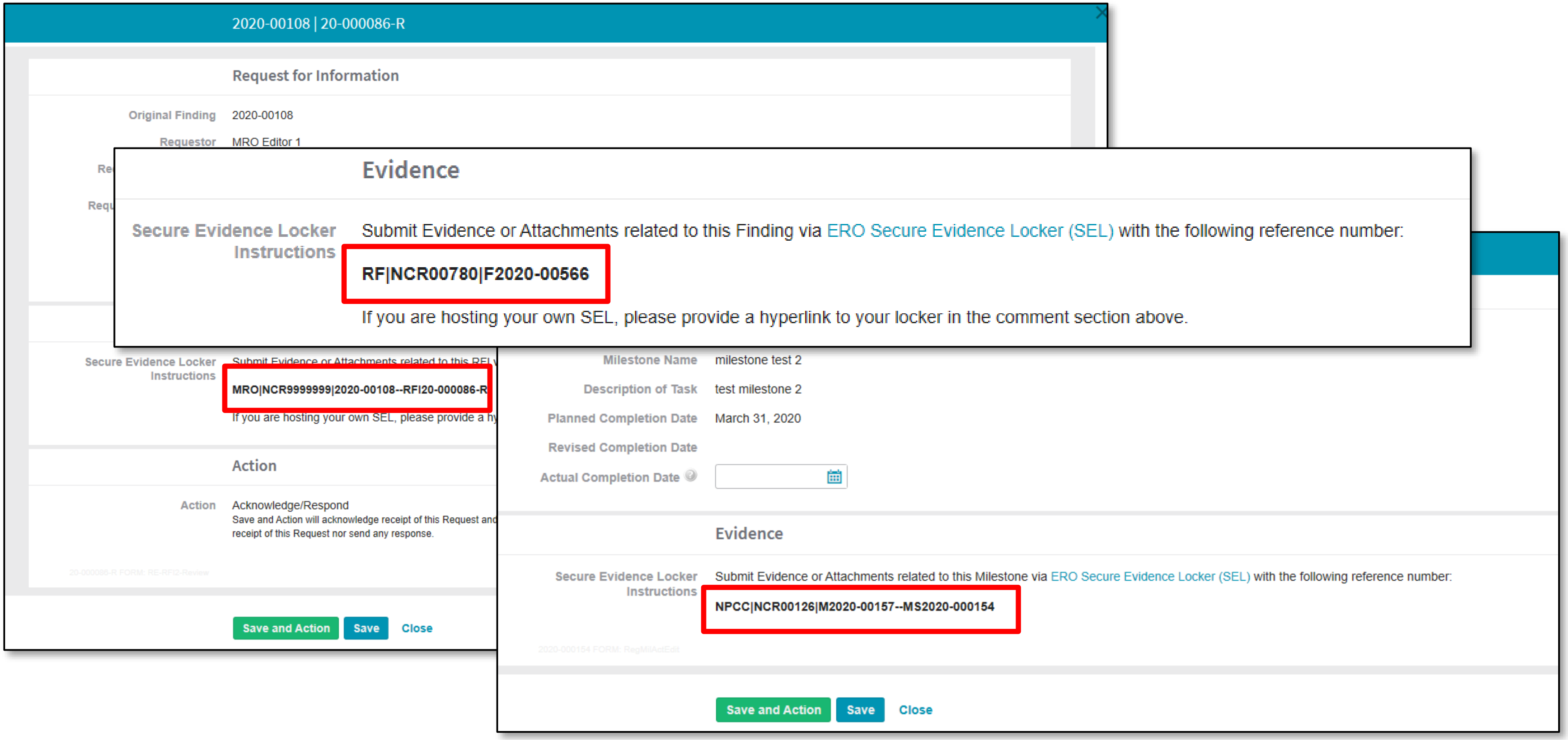
This is a North American Electric Reliability Corporation (NERC) information system restricte
You have no reasonable expectation of privacy regarding communications or data tran
information system. At any time and for any lawful purpose, NERC may monitor, interce
communications or data transiting or stored on this information system. At NERC's sole di
pertinent information to the U.S. Government and its authorized representatives to pro
infrastructure and key resources, ensure information security, or to comply with any appli
process, or enforceable governmental request. By continuing, you acknowledge that you un
terms and conditions described in this notice. The actual or attempted unauthorized access,
system is strictly prohibited and may subject violators to criminal, civil, and/or administrative

For security reasons, we require additional information to verify your account

Pushed a login request to your device...

ERO SEL – Registered Entity Experience

- Align will provide reference numbers for use when uploading to the Secure Evidence Locker



2020-00108 | 20-000086-R

Request for Information

Original Finding 2020-00108

Requestor MRO Editor 1

Re

Requ

Secure Evidence Locker Instructions Submit Evidence or Attachments related to this RFI v

MRO|NCR9999999|2020-00108--RFI20-000086-R

If you are hosting your own SEL, please provide a hy

Action

Action Acknowledge/Respond
Save and Action will acknowledge receipt of this Request and
receipt of this Request nor send any response.

20-000086-R FORM: RE-RFI2-Review

Evidence

Secure Evidence Locker Instructions Submit Evidence or Attachments related to this Finding via ERO Secure Evidence Locker (SEL) with the following reference number:

RF|NCR00780|F2020-00566

If you are hosting your own SEL, please provide a hyperlink to your locker in the comment section above.

Milestone Name milestone test 2

Description of Task test milestone 2

Planned Completion Date March 31, 2020

Revised Completion Date

Actual Completion Date

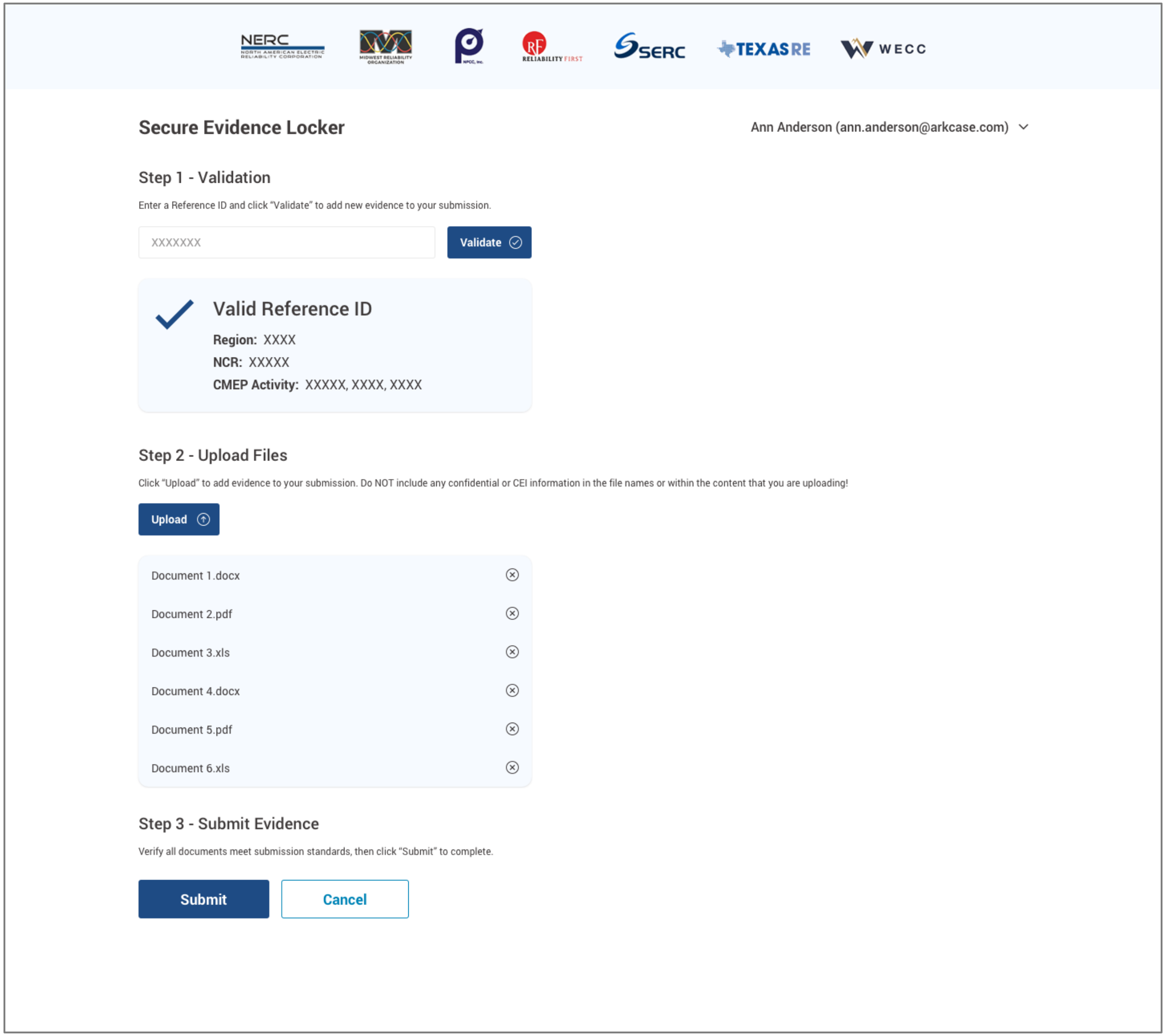
Evidence

Secure Evidence Locker Instructions Submit Evidence or Attachments related to this Milestone via ERO Secure Evidence Locker (SEL) with the following reference number:

NPCC|NCR00126|M2020-00157--MS2020-000154

2020-000154 FORM: RegMilActEdit

ERO SEL – Registered Entity Experience



Secure Evidence Locker

Ann Anderson (ann.anderson@arkcase.com)

Step 1 - Validation

Enter a Reference ID and click "Validate" to add new evidence to your submission.

XXXXXXX

Validate

✓ Valid Reference ID

Region: XXXX

NCR: XXXXX

CMEP Activity: XXXXX, XXXX, XXXX

Step 2 - Upload Files

Click "Upload" to add evidence to your submission. Do NOT include any confidential or CEI information in the file names or within the content that you are uploading!

Upload

Document 1.docx ⊗

Document 2.pdf ⊗

Document 3.xls ⊗

Document 4.docx ⊗

Document 5.pdf ⊗

Document 6.xls ⊗

Step 3 - Submit Evidence

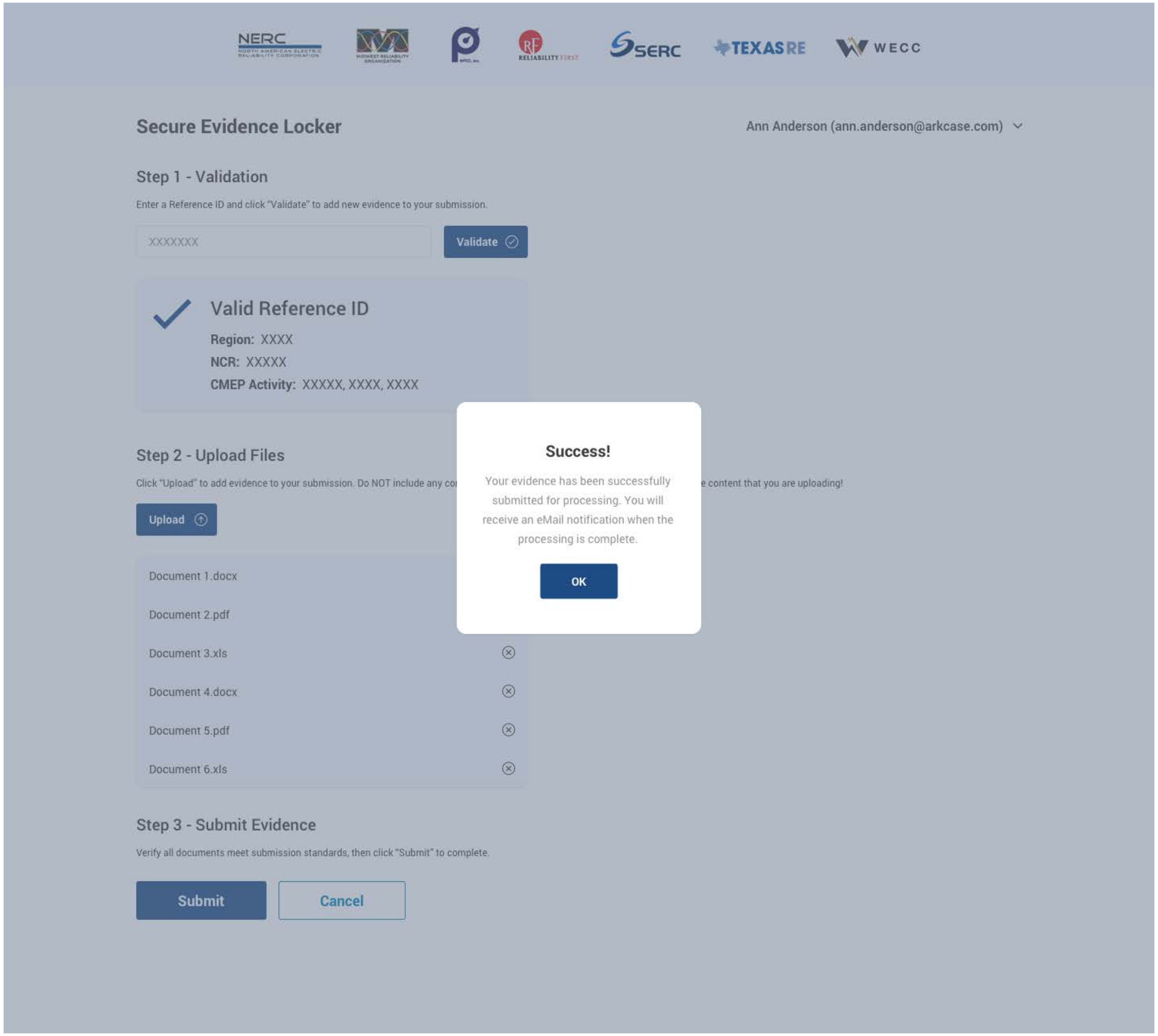
Verify all documents meet submission standards, then click "Submit" to complete.

Submit

Cancel

- Enter reference ID and click Validate
- Upload Files(s)
- Click Submit

ERO SEL – Registered Entity Experience



Secure Evidence Locker

Ann Anderson (ann.anderson@arkcase.com)

Step 1 - Validation

Enter a Reference ID and click "Validate" to add new evidence to your submission.

XXXXXXX

Validate

✓ Valid Reference ID

Region: XXXX

NCR: XXXXX

CMEP Activity: XXXXX, XXXX, XXXX

Step 2 - Upload Files

Click "Upload" to add evidence to your submission. Do NOT include any co e content that you are uploading!

Upload

Document 1.docx

Document 2.pdf

Document 3.xls

Document 4.docx

Document 5.pdf

Document 6.xls

Step 3 - Submit Evidence

Verify all documents meet submission standards, then click "Submit" to complete.

Submit

Cancel

Success!

Your evidence has been successfully submitted for processing. You will receive an eMail notification when the processing is complete.

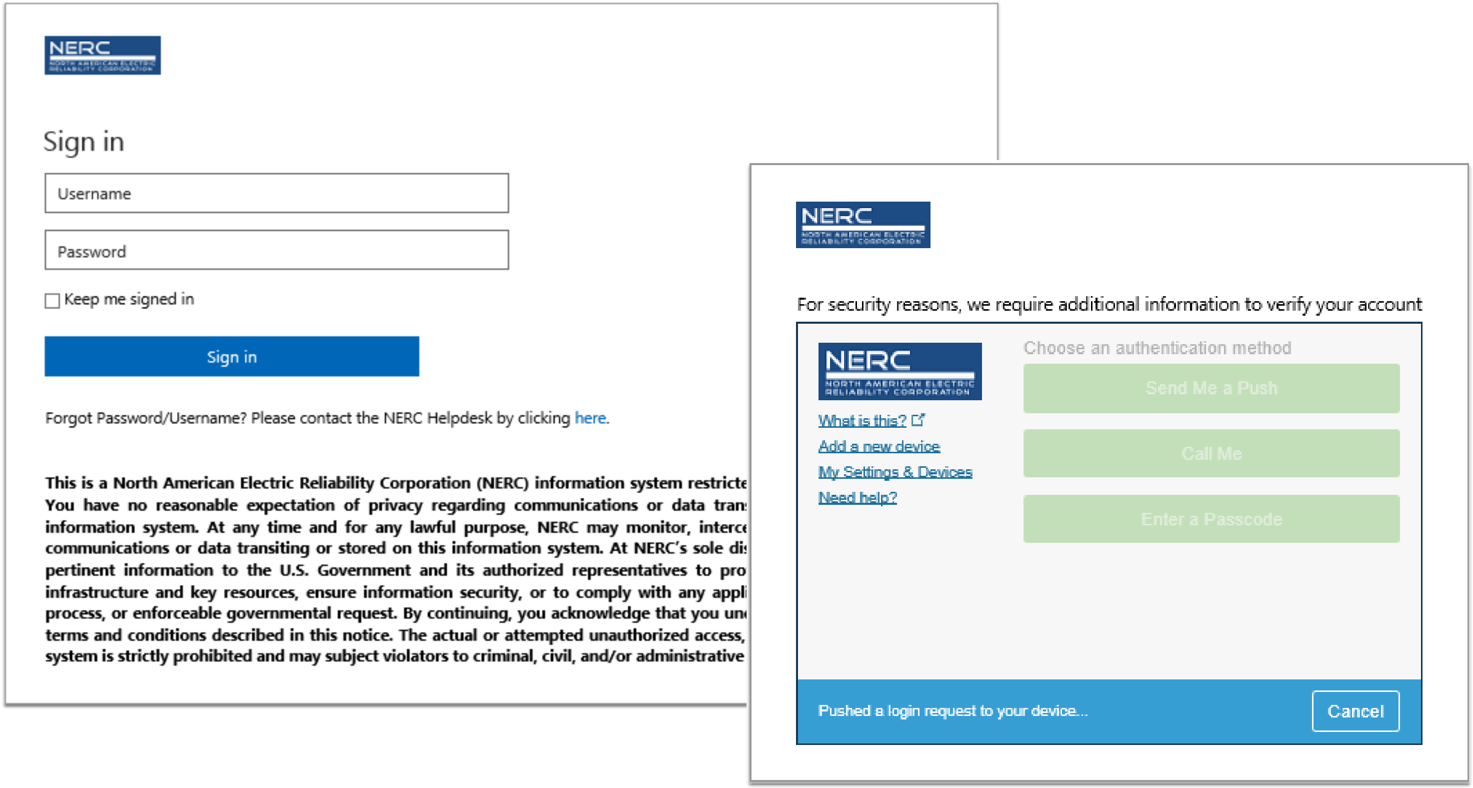
OK

- Multiple files can be uploaded at once
- Receive email confirmation of submission, including “Hash Value,” to ensure submission integrity

Regional Entity Experience

ERO SEL – Regional Entity Experience

- Users will log into the Secure Evidence Locker through a URL and be authenticated using their ERO Portal account with MFA



Sign in

Username

Password

□ Keep me signed in

Forgot Password/Username? Please contact the NERC Helpdesk by clicking here.

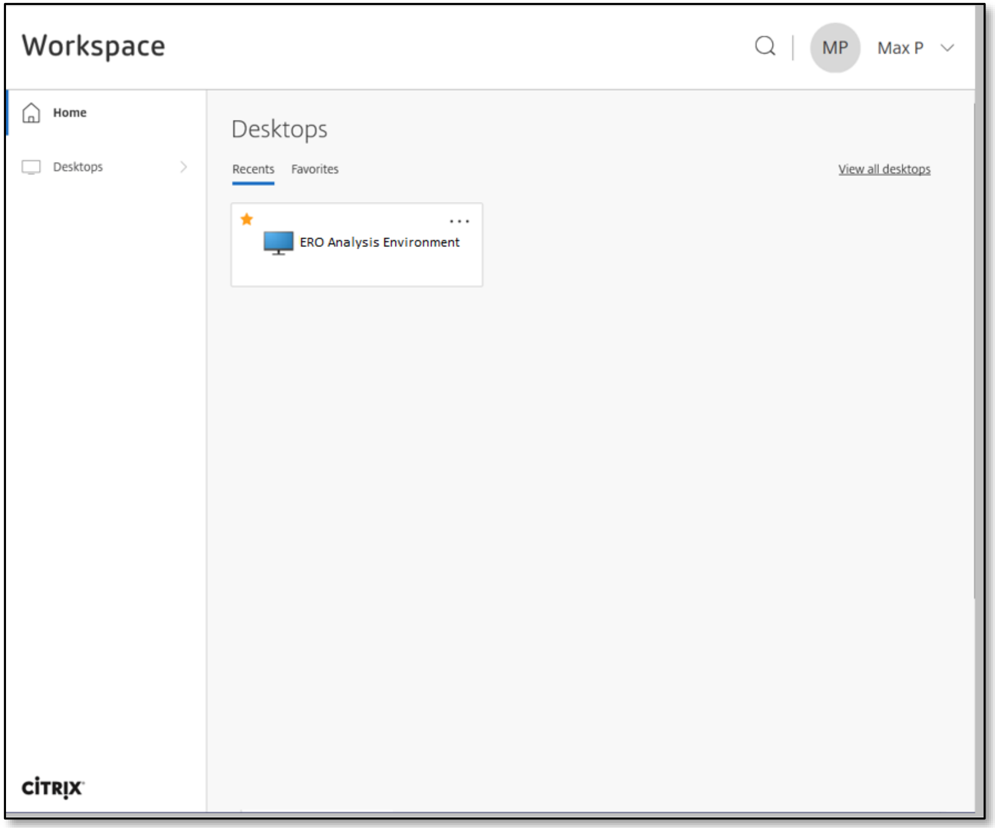
This is a North American Electric Reliability Corporation (NERC) information system restricte
You have no reasonable expectation of privacy regarding communications or data tran
information system. At any time and for any lawful purpose, NERC may monitor, interc
communications or data transiting or stored on this information system. At NERC's sole di
pertinent information to the U.S. Government and its authorized representatives to pro
infrastructure and key resources, ensure information security, or to comply with any appli
process, or enforceable governmental request. By continuing, you acknowledge that you un
terms and conditions described in this notice. The actual or attempted unauthorized access,
system is strictly prohibited and may subject violators to criminal, civil, and/or administrative

For security reasons, we require additional information to verify your account

Pushed a login request to your device...

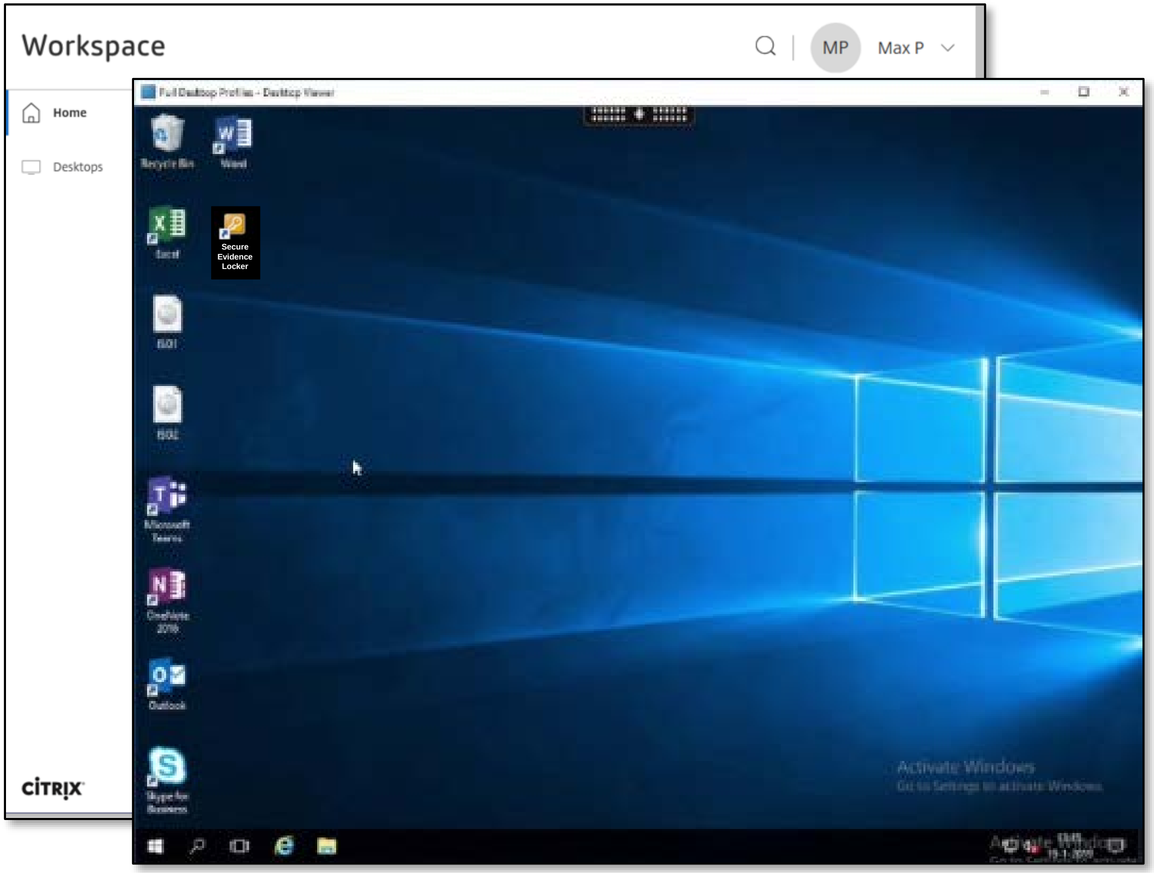
ERO SEL – Regional Entity Experience

- Once logged in, users will be presented with a workspace, which will provide the ability to launch an ERO Analysis Environment



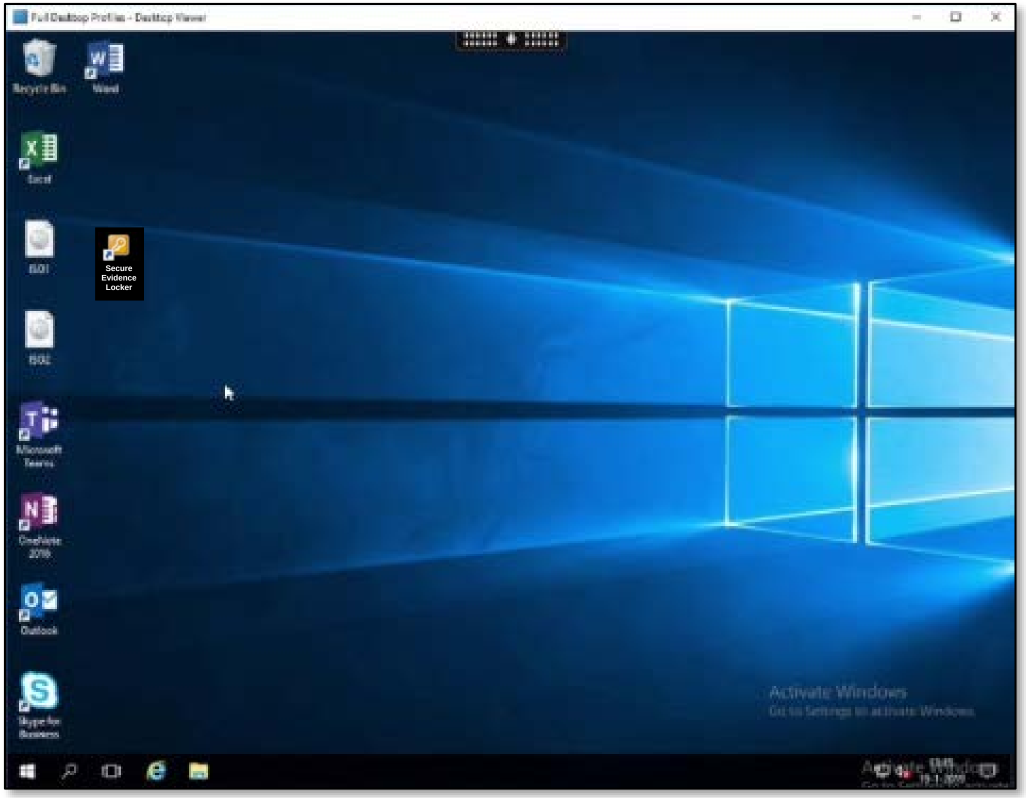
ERO SEL – Regional Entity Experience

- Once the user clicks on ‘ERO Analysis Environment,’ a new desktop environment will launch

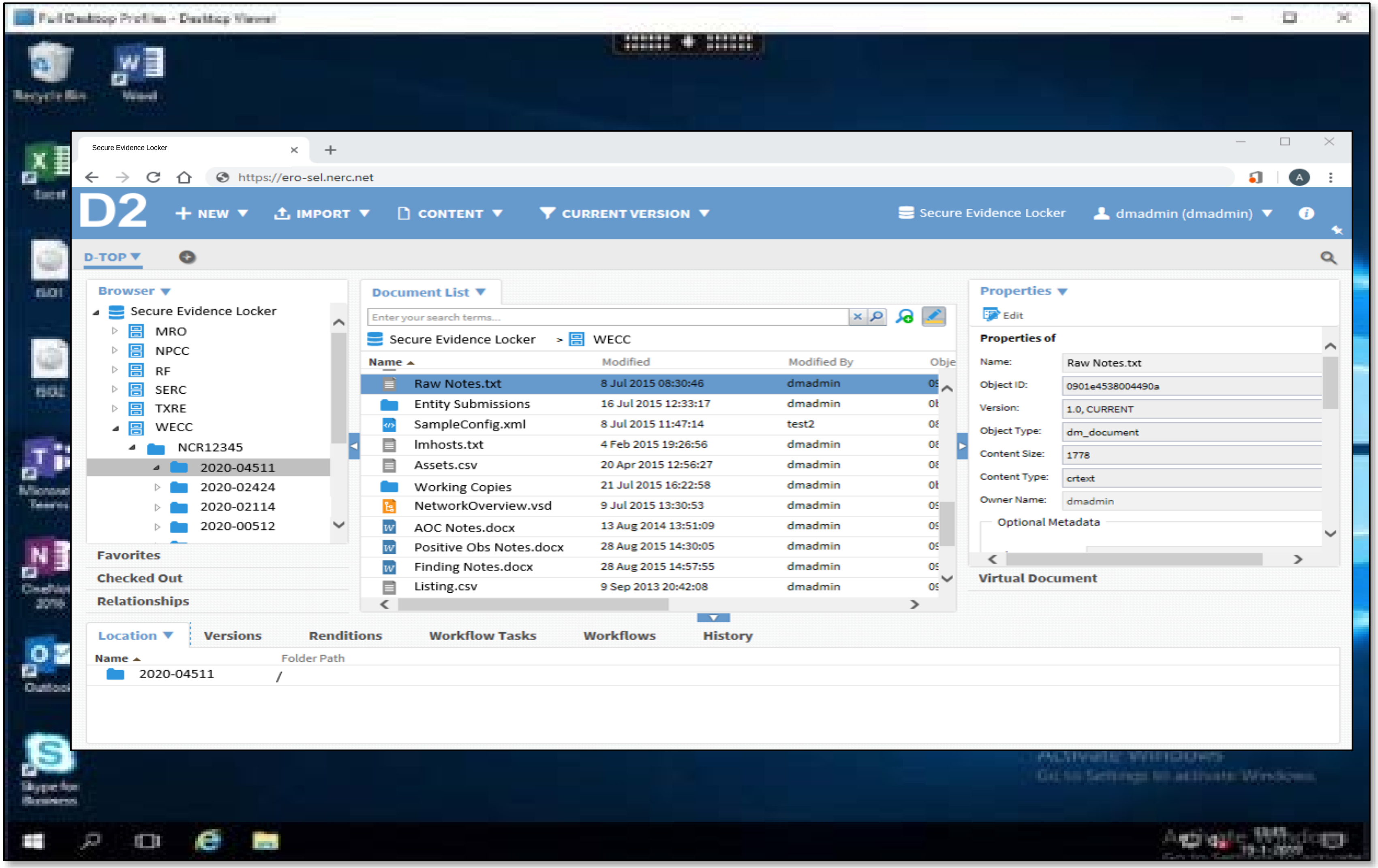


ERO SEL – Regional Entity Experience

- This environment is a fully-functioning Windows environment, loaded with all the applications required to analyze submitted evidence, including MS Office, Adobe Acrobat, NP-View, etc.
- Clicking on the ‘Secure Evidence Locker’ icon will launch the Locker within the desktop environment



ERO SEL – Regional Entity Experience



Name	Modified	Modified By	Obje
Raw Notes.txt	8 Jul 2015 08:30:46	dmadmin	09
Entity Submissions	16 Jul 2015 12:33:17	dmadmin	0b
SampleConfig.xml	8 Jul 2015 11:47:14	test2	08
lmhosts.txt	4 Feb 2015 19:26:56	dmadmin	08
Assets.csv	20 Apr 2015 12:56:27	dmadmin	08
Working Copies	21 Jul 2015 16:22:58	dmadmin	0b
NetworkOverview.vsd	9 Jul 2015 13:30:53	dmadmin	09
AOC Notes.docx	13 Aug 2014 13:51:09	dmadmin	09
Positive Obs Notes.docx	28 Aug 2015 14:30:05	dmadmin	09
Finding Notes.docx	28 Aug 2015 14:57:55	dmadmin	09
Listing.csv	9 Sep 2013 20:42:08	dmadmin	09

Properties of

Name:	Raw Notes.txt
Object ID:	0901e4538004490a
Version:	1.0, CURRENT
Object Type:	dm_document
Content Size:	1778
Content Type:	crtext
Owner Name:	dmadmin

Name	Folder Path
2020-04511	/

ERO SEL – Regional Entity Experience

- In order to exit, the user will, first, close the Secure Evidence Locker window then log out of the desktop environment
- Any work left on in the Analysis Environment will be destroyed when logging out

ERO SEL Potential Risks

- Support of new technologies
- Delays created by the COVID-19 pandemic
  - Professional Services (travel and collaboration)
  - Testing and in-person training

Questions and Answers