NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technology and Security Committee (TSC) Open Meeting Presentations

November 4, 2020

RELIABILITY | RESILIENCE | SECURITY

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Operations Update

Manny Cancel
Technology and Security Committee Meeting
November 4, 2020

TLP:WHITE

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Operations Update
- Threat Landscape
- Strategic Partnerships
- GridEx VI
- Policy Input
  - Feedback
  - Outreach
  - Next Steps

Operations Update

- E-ISAC continues to operate remotely and develop responsible return plans
- Organization changes
- ESCC activities
- Executive Order 13920
- Cross-sector coordination with other ISACs, Analysis and Resiliency Center (ARC)
- 20% increase in membership and 37% increase in portal users
- Portal Upgrade scheduled for January 2021
- CIP-008 reporting goes into effect on January 1, 2021

Threat Landscape: Cybersecurity

- Key Advanced Persistent Threat (APT) groups tracked:
  - Russia: Sandworm Team and associated APT28
  - China: APT10 and APT41
- Trends and Observations
  - Potential for Ransomware impact to OT systems
  - Emotet malware not seen in sector, prevalent in SLTT and elections

Threat Landscape: Physical Security

- Trends
  - 29% increase in intrusions
  - 103% increase in vandalism
  - 55% increase in gunfire incidents
  - Civil unrest
  - Increased surveillance activities using unmanned aircraft systems (drones)
- Products
  - Physical Security Reports
  - Wind Farm Security White Paper
  - Protective Measures Index Tool
  - Security vulnerability assessment workshop (VISA Workshop)
  - E-ISAC Situational Awareness Summary: 2020 Election

Strategic Partnerships

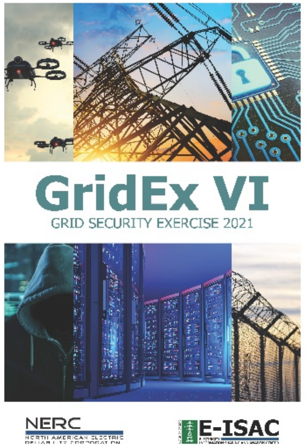
- DOE
  - Coordinating on OT initiatives, CRISP OT pilot, Essence OT pilot
  - ESCC unclassified threat briefing
  - GridEx VI
- DHS
  - Intelligence reports derived from E-ISAC Portal posts
  - Advance notifications on Malware Analysis Reports
  - Update CISA on outages and threats to the bulk power system to support 2020 elections
- MS-ISAC/EL-ISAC
  - Coordinating with MS/EI-ISAC to inform industry election security

Strategic Partnerships

- Canadian Partnerships
  - Canadian Electricity Association
  - Canadian Security Establishment’s EnerSEcCC
  - IESO
- Analysis & Resilience Center (formerly FSARC)
  - Developing formal collaboration agreement
  - Participated in Energy Risk Committee meeting

GridEx VI

- Exercise the resilience of the North American electricity system in the face of a coordinated attack from a state-sponsored adversary
  - Distributed Play - November 16-17, 2021
  - Executive Tabletop - November 18, 2021
- Hagerty Consulting awarded contract
- Potential scenarios include kinetic attacks, social engineering, supply chain, insider threat, cross-sector impacts, etc.



Policy Input Feedback

- Stakeholders are generally supportive of strategy
- Common themes:
  - Support Canadian objectives
  - Minimize duplication of efforts with other initiatives and programs
  - Ensure fiscal responsibility and cost efficiency
  - Operate within E-ISAC mandate/scope
  - Clarify objectives and deliverables of major programs
  - Ensure extension of services does not erode services to electricity industry or increase costs
  - Evaluate implementation timeframes
  - Evaluate cross-sector activities

Policy Input Outreach

- Contacted respondents for clarification and ensured no additional concerns needed to be addressed
- Outreach to Trade Associations and NERC Member Representatives Committee

Policy Input Next Steps

- Update strategic plan to address feedback
- Update NERC Board
- Continue outreach to membership, trade associations and regions
- Track progress on strategic plan initiatives on quarterly basis

Questions and Answers

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Business Technology Projects Update

Stan Hoptroff, Vice President, Business Technology
Technology and Security Committee Meeting
November 4, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

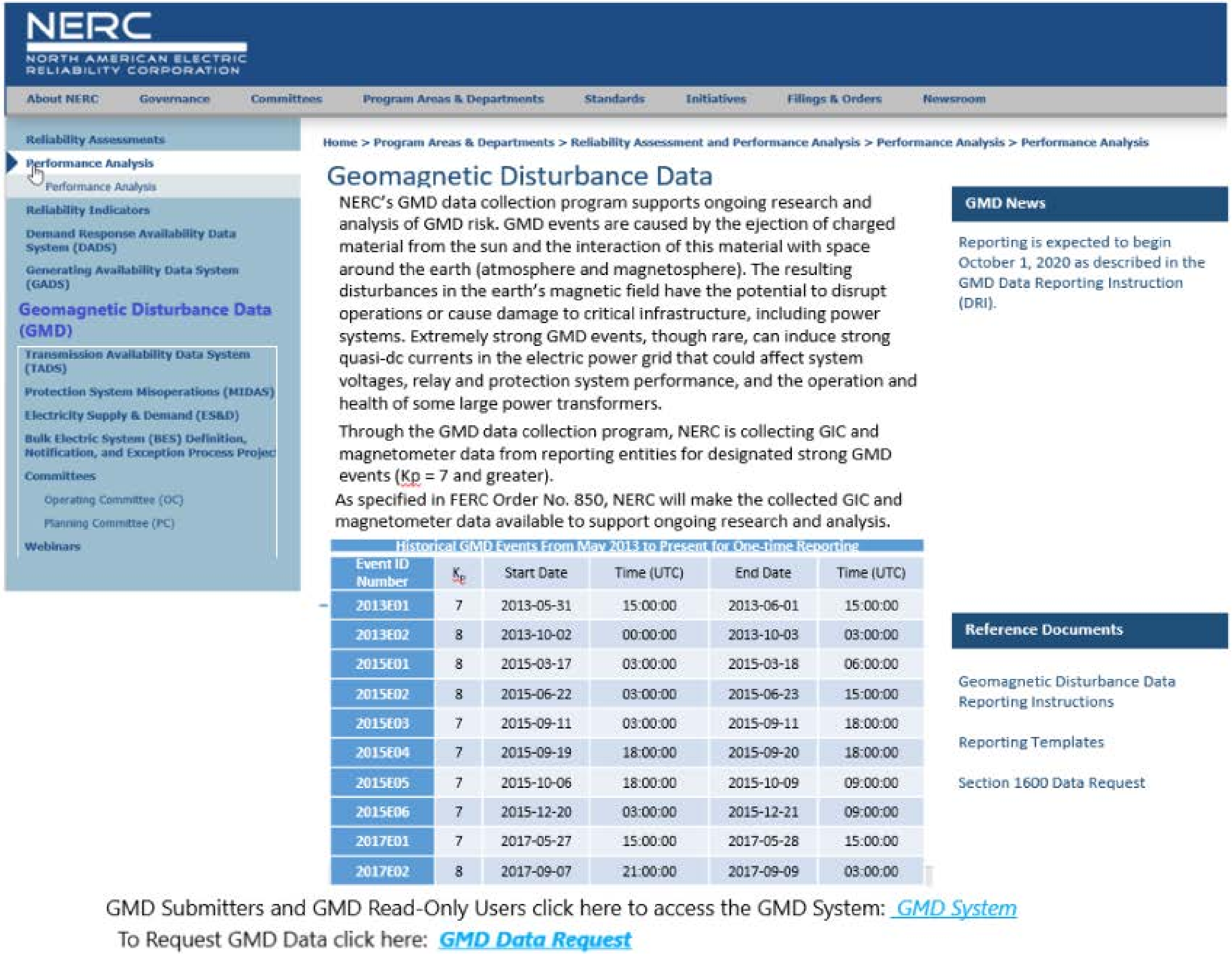
- ERO Business Technology Projects Update
  - Geomagnetic Disturbance (GMD) application
  - Microsoft TEAMS Collaboration Platform
- Electricity Information Sharing and Analysis Center (E-ISAC) Technology Projects
  - Salesforce customer relationship management (CRM)
- Security Advisory Group
- Priorities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

GMD

- Section 1600 Data Request; FERC Order 830
- October 1, 2020 released to production
- 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	Kp	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).

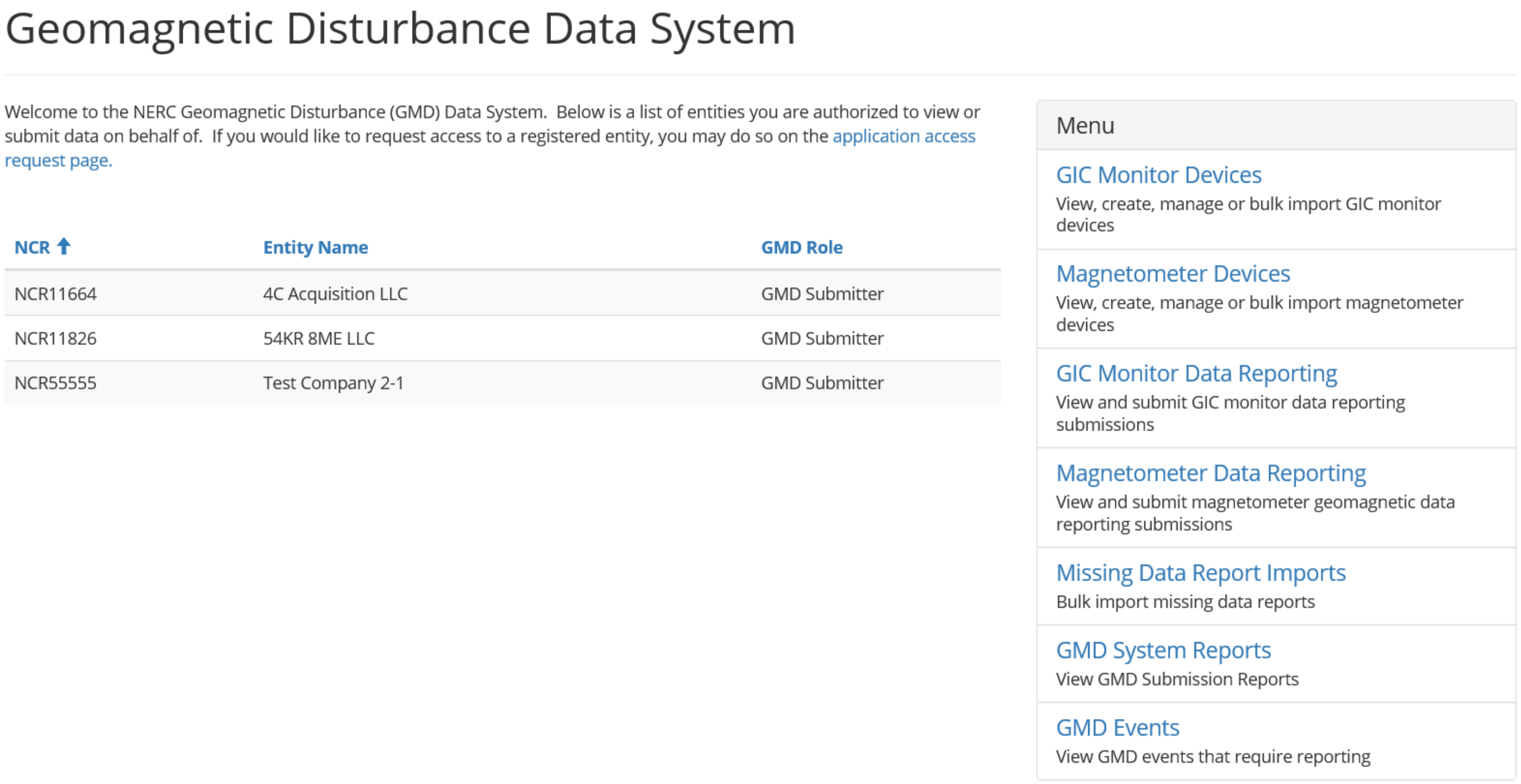
Reference Documents

Geomagnetic Disturbance Data Reporting Instructions

Reporting Templates

Section 1600 Data Request

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

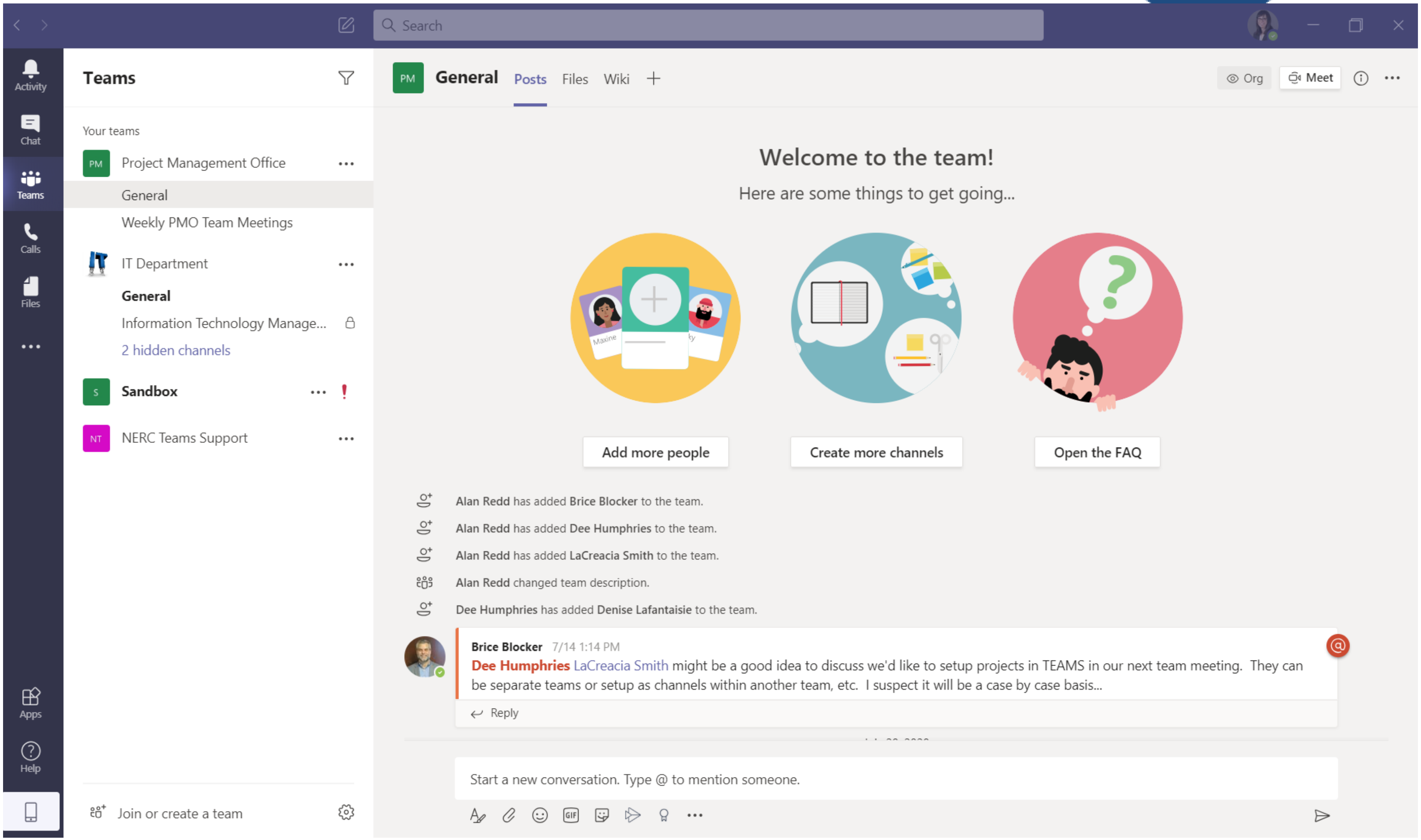
GMD Business Readiness

- 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 is complete
  - Data reporting training sessions are in progress – October 2020
  - Data Researcher training will be delayed until 2021 to allow for a period of data collection in Q4 2020

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
- 80M global users

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

Security Advisory Group

- Advisory body established by NERC Management
- Represents all industry sectors; engagement at the Chief Information Security Officer level
- Will interface with NERC IT Leadership
- Supports NERC Management with expertise and advice on data confidentiality, integrity and security
- Sensitive industry information stored or processed by NERC

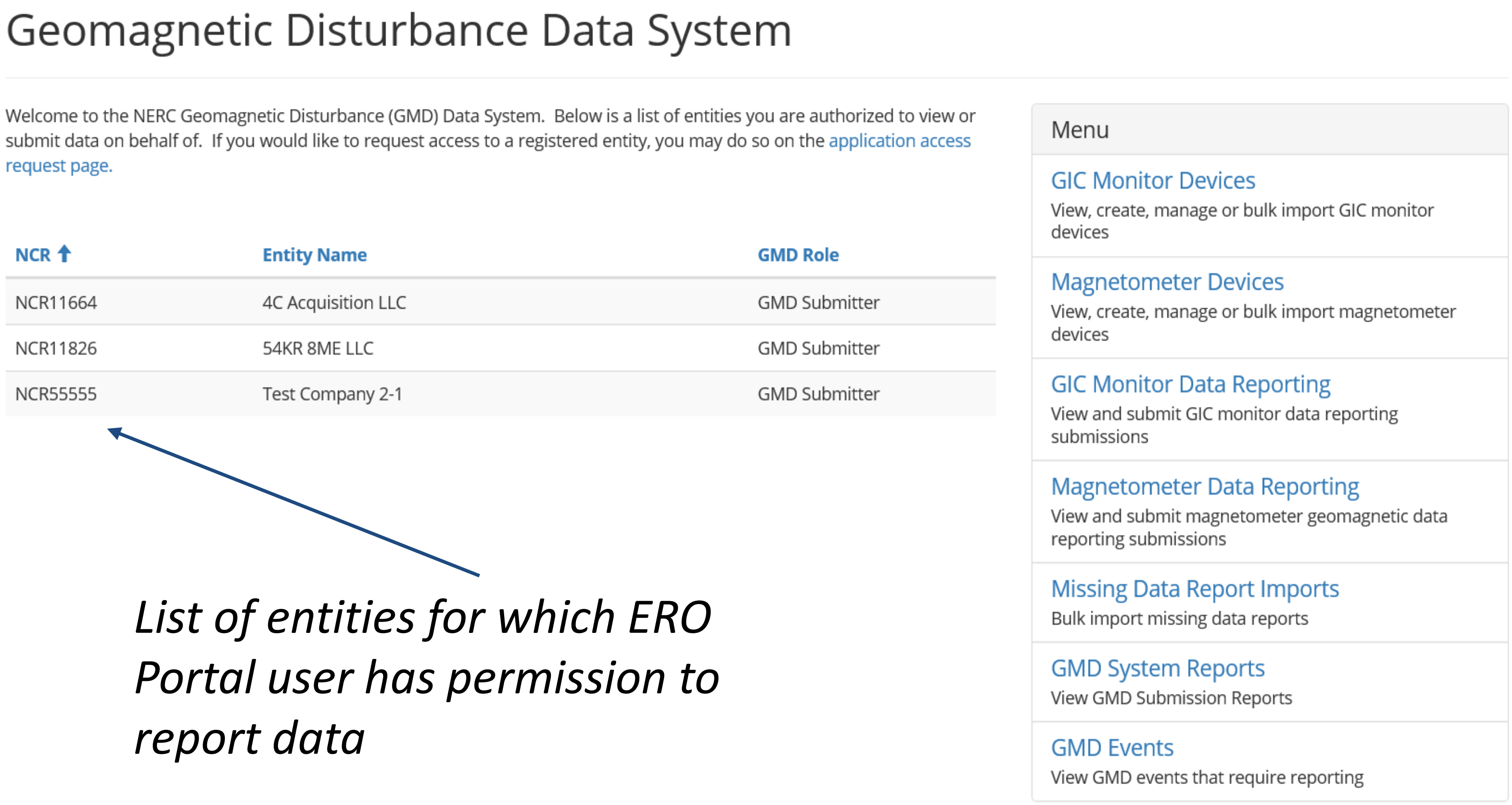
Priorities Looking Ahead

- 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

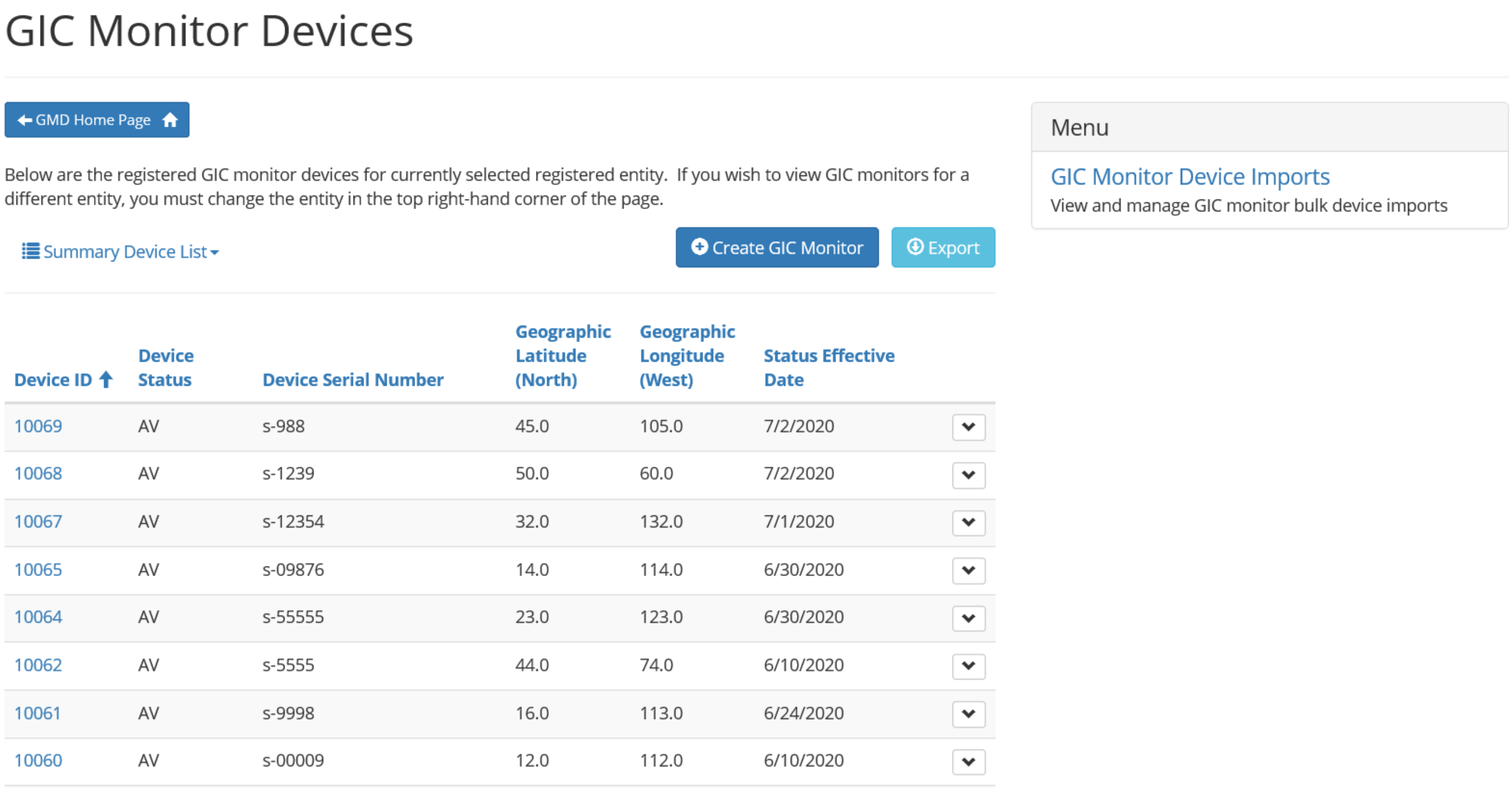
GMD System Reports
View GMD Submission Reports

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



GIC Monitor Devices

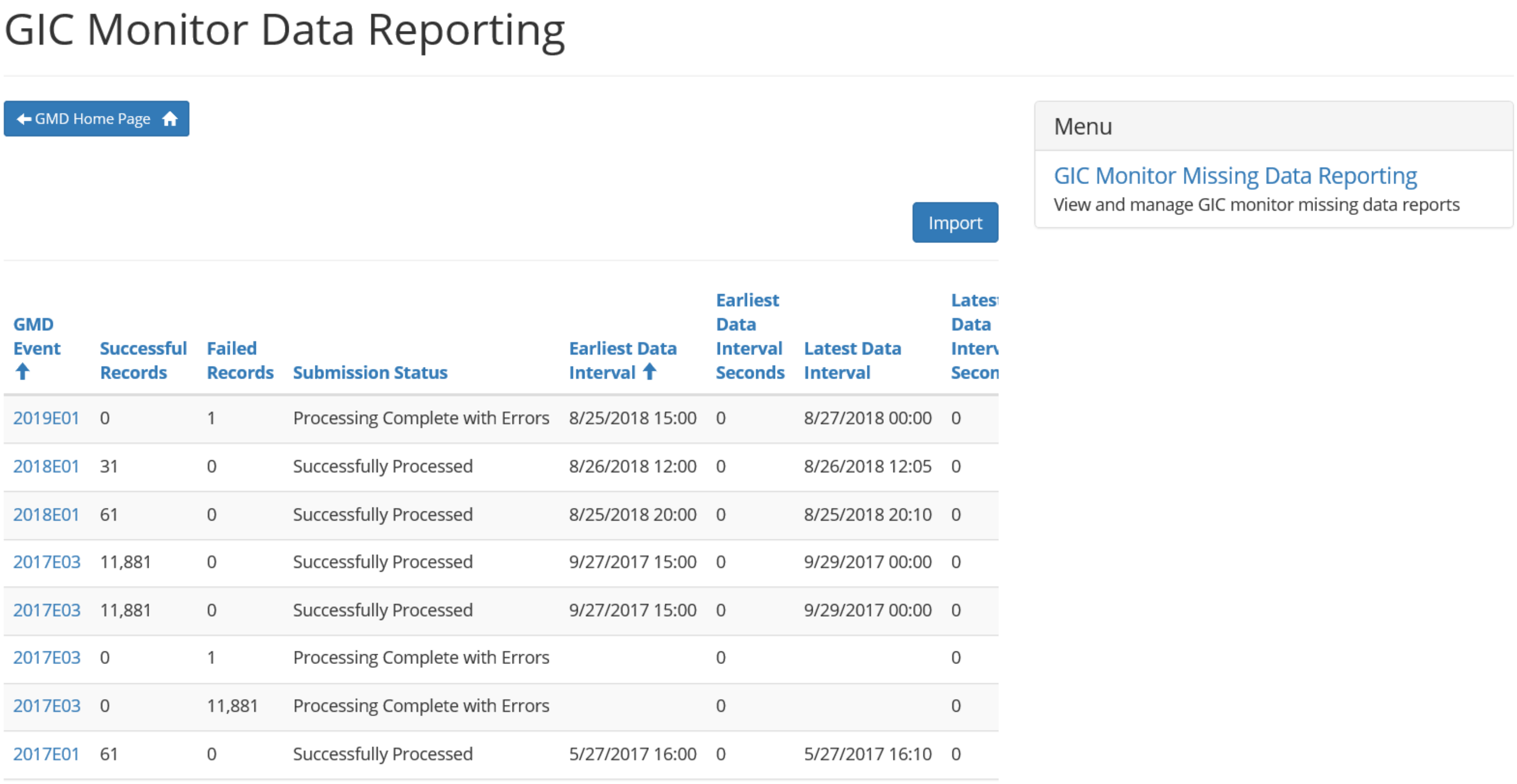
Below are the registered GIC monitor devices for currently selected registered entity. If you wish to view GIC monitors for a different entity, you must change the entity in the top right-hand corner of the page.

GIC Monitor Device Imports
View and manage GIC monitor bulk device imports

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



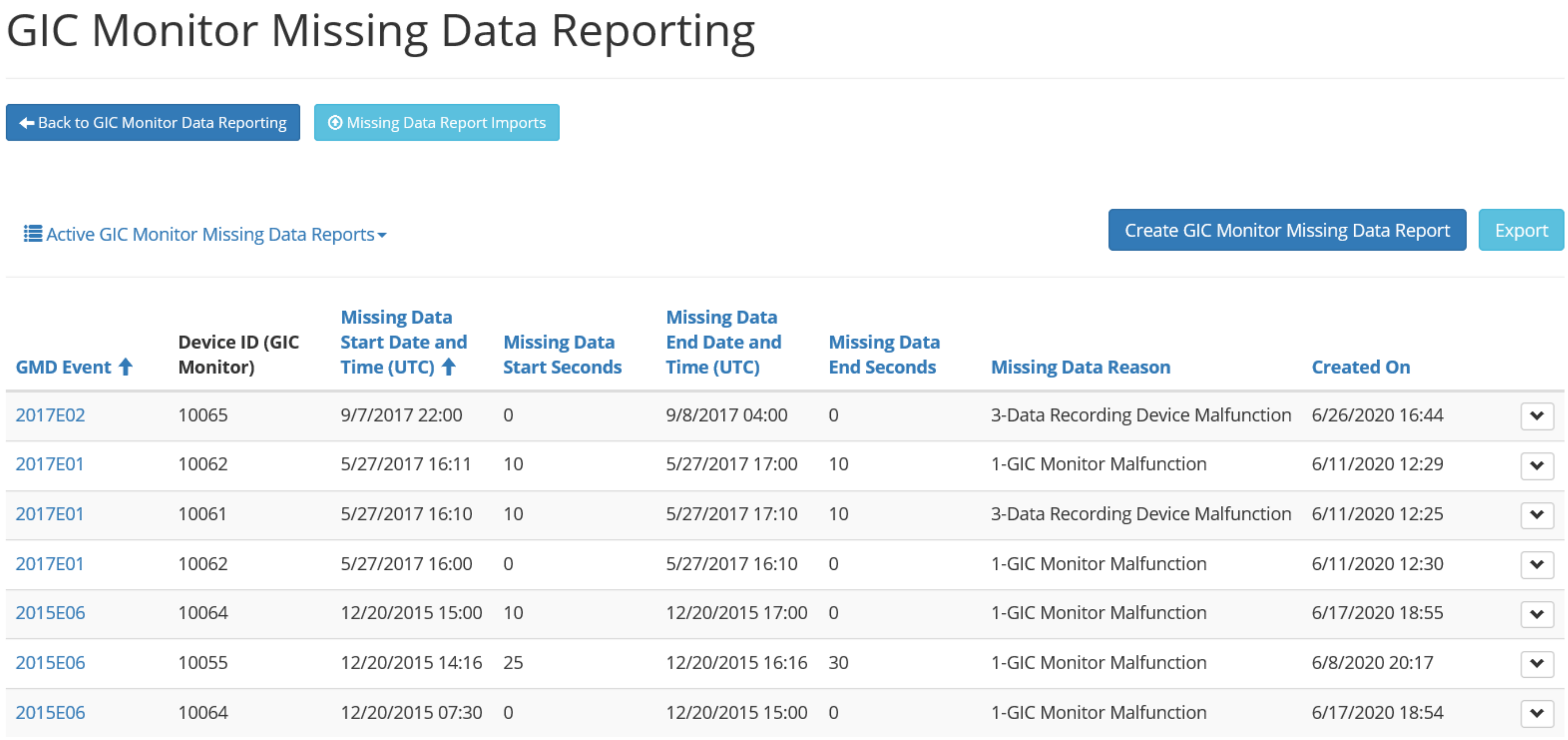
GIC Monitor Data Reporting

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



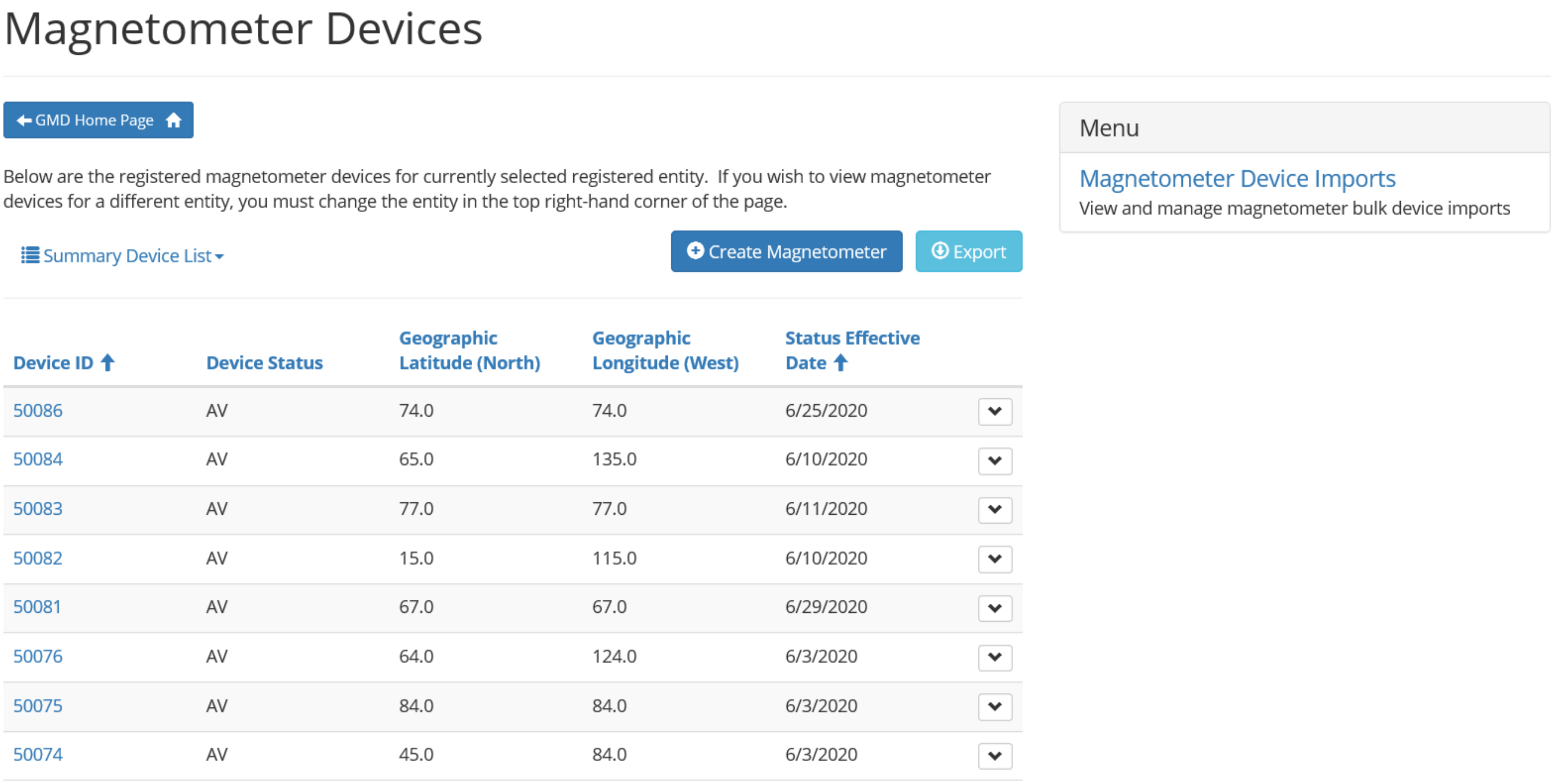
GIC Monitor Missing Data Reporting

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

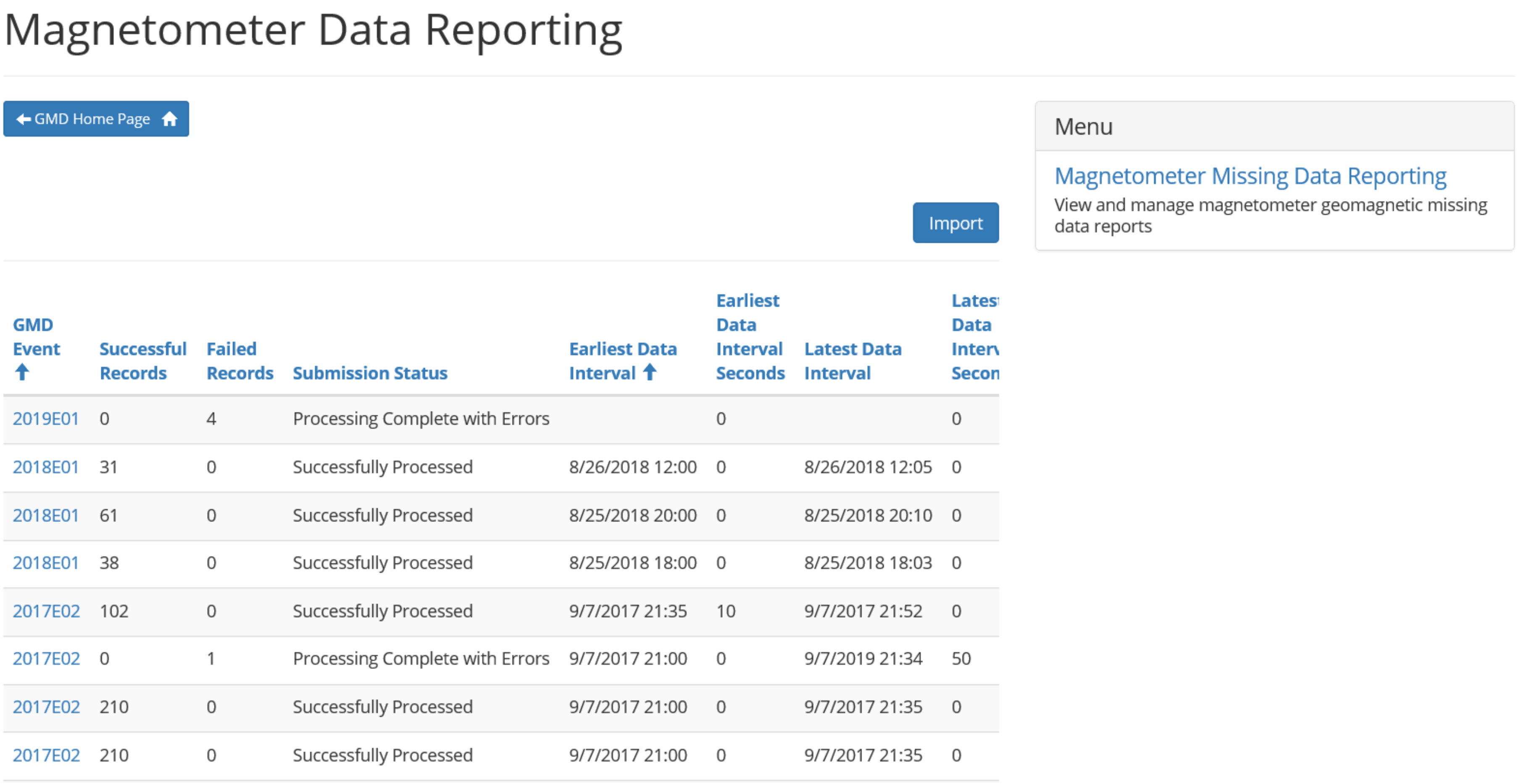
Below are the registered magnetometer devices for currently selected registered entity. If you wish to view magnetometer devices for a different entity, you must change the entity in the top right-hand corner of the page.

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

View and manage magnetometer bulk device imports

Magnetometer Data Reporting

- Magnetometer Device Import Validation Results



Magnetometer Data Reporting

Menu

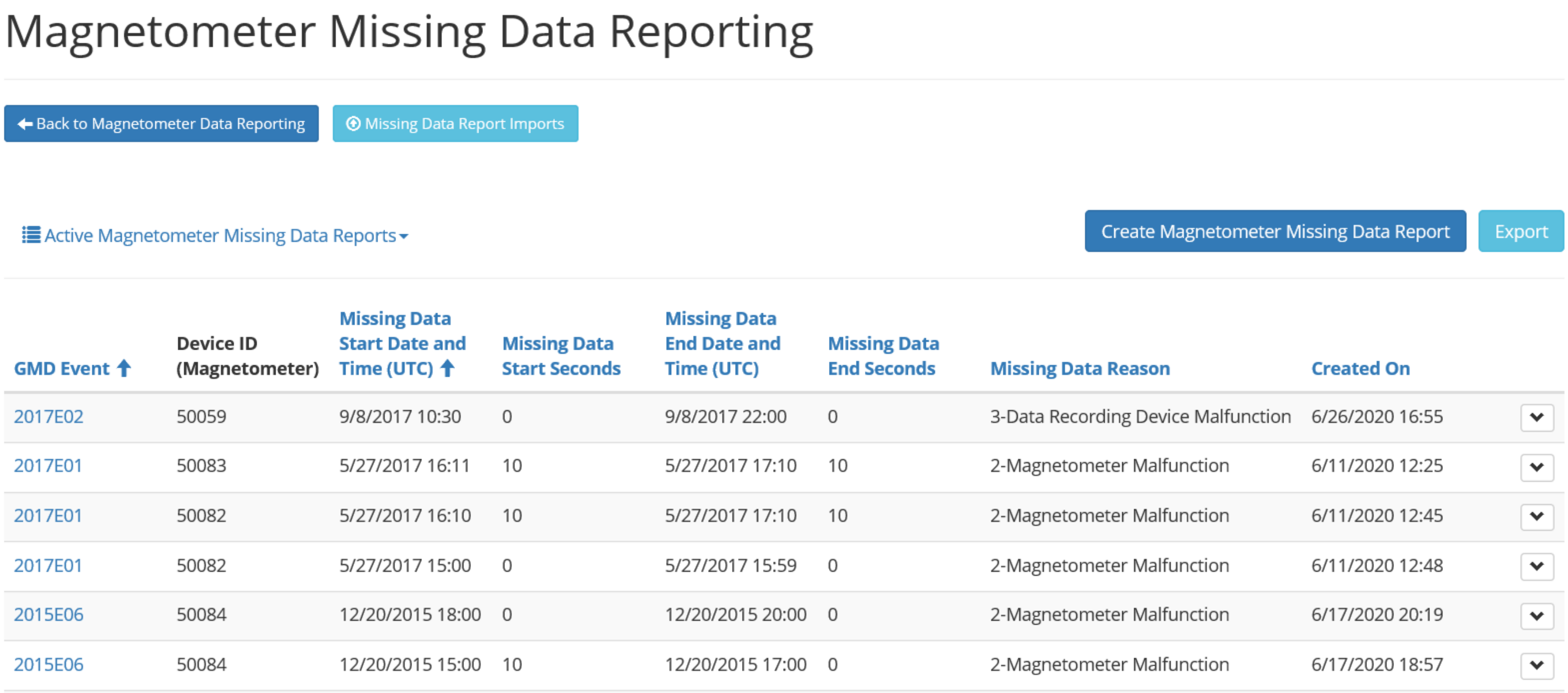
Magnetometer Missing Data Reporting

View and manage magnetometer geomagnetic 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	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

Magnetometer Missing Data Reporting

- Missing Data Reports Document Gaps in GMD Event Data



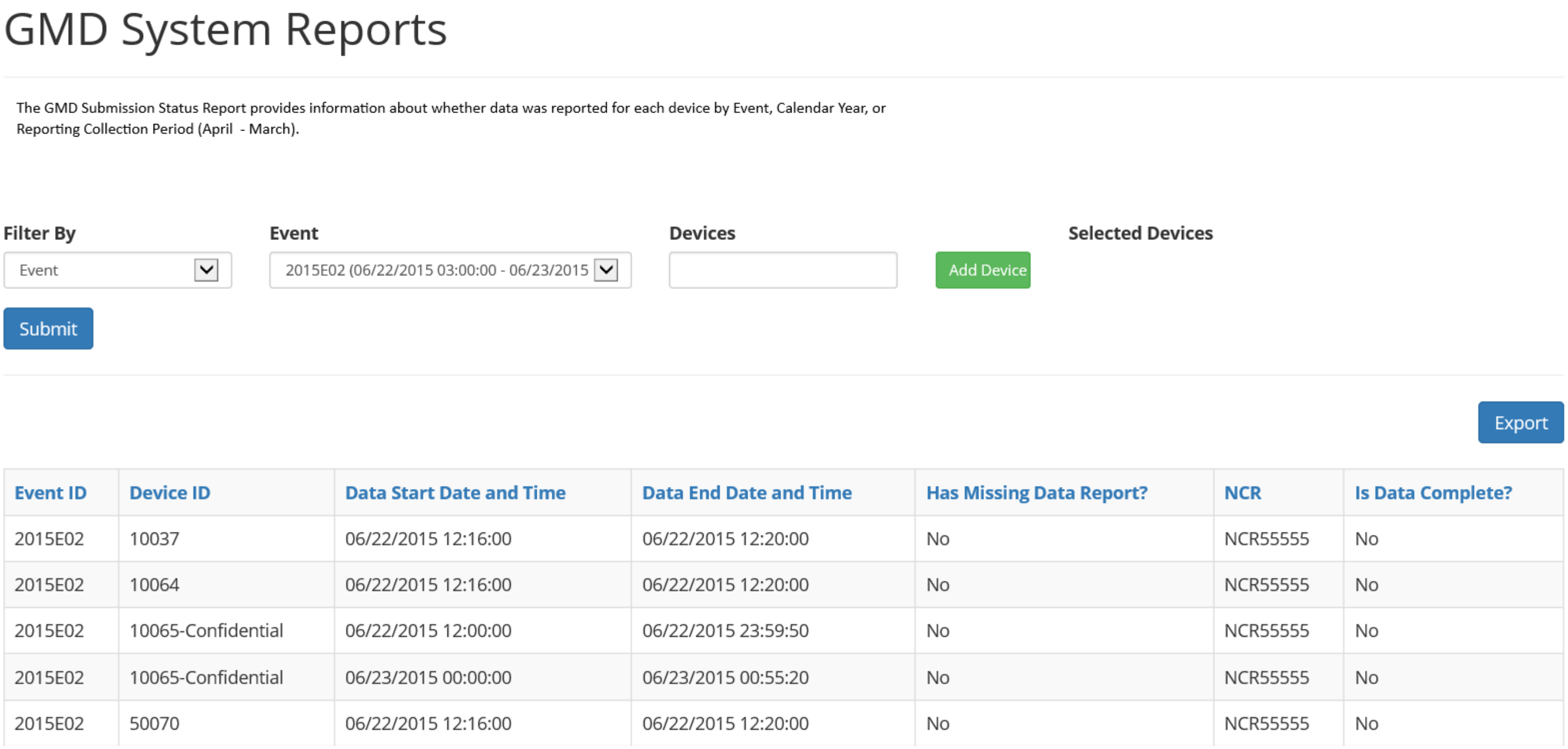
Magnetometer Missing Data Reporting

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

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

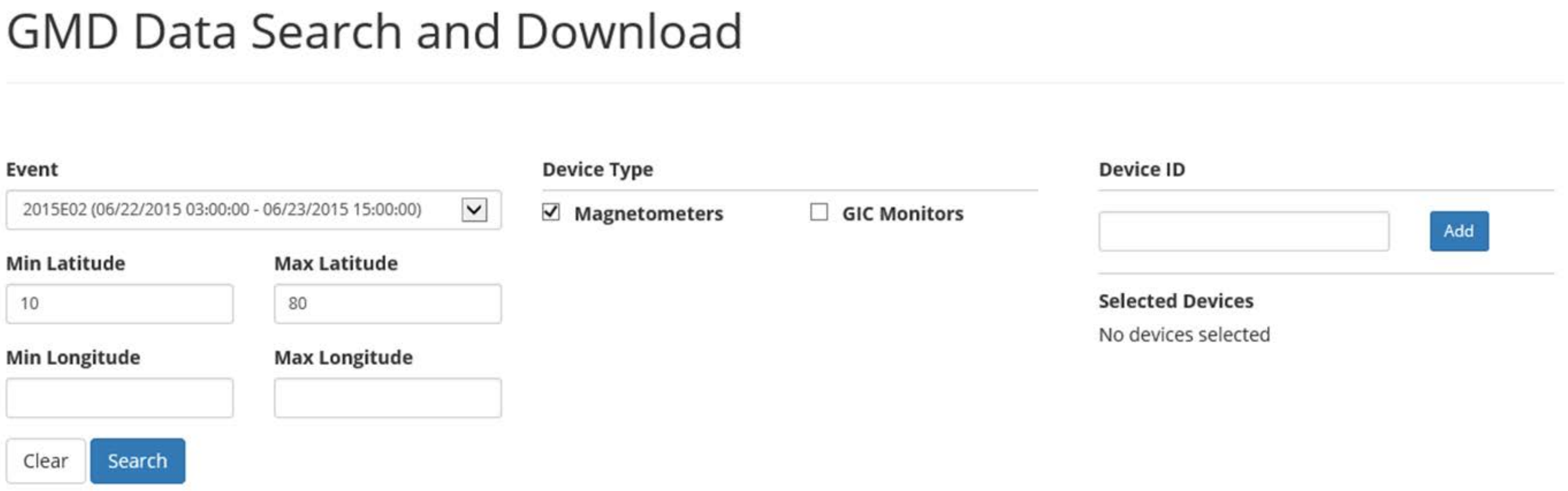
Devices:

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

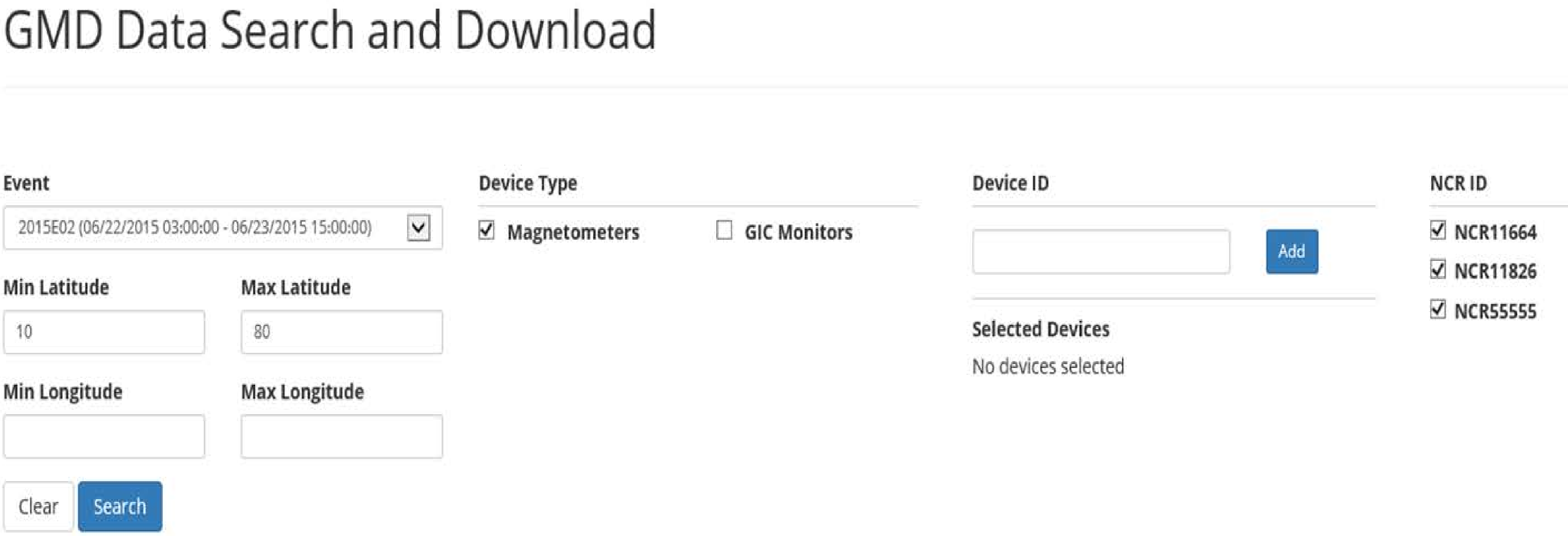
Device Type
☑ Magnetometers ☐ GIC Monitors

Device ID

Selected Devices
No devices selected

GMD Data Search and Download

- GMD Data Submitters Also Can Search by Entity NERC Compliance Registry 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

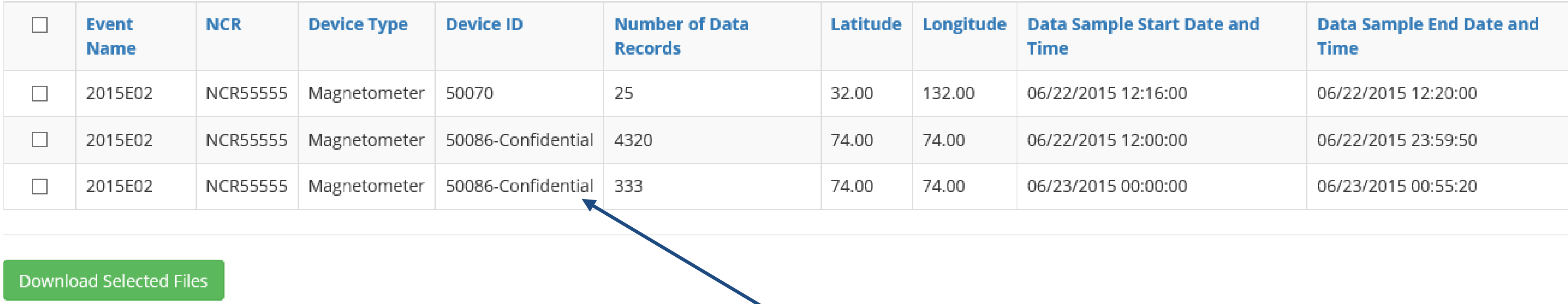
Device ID:

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

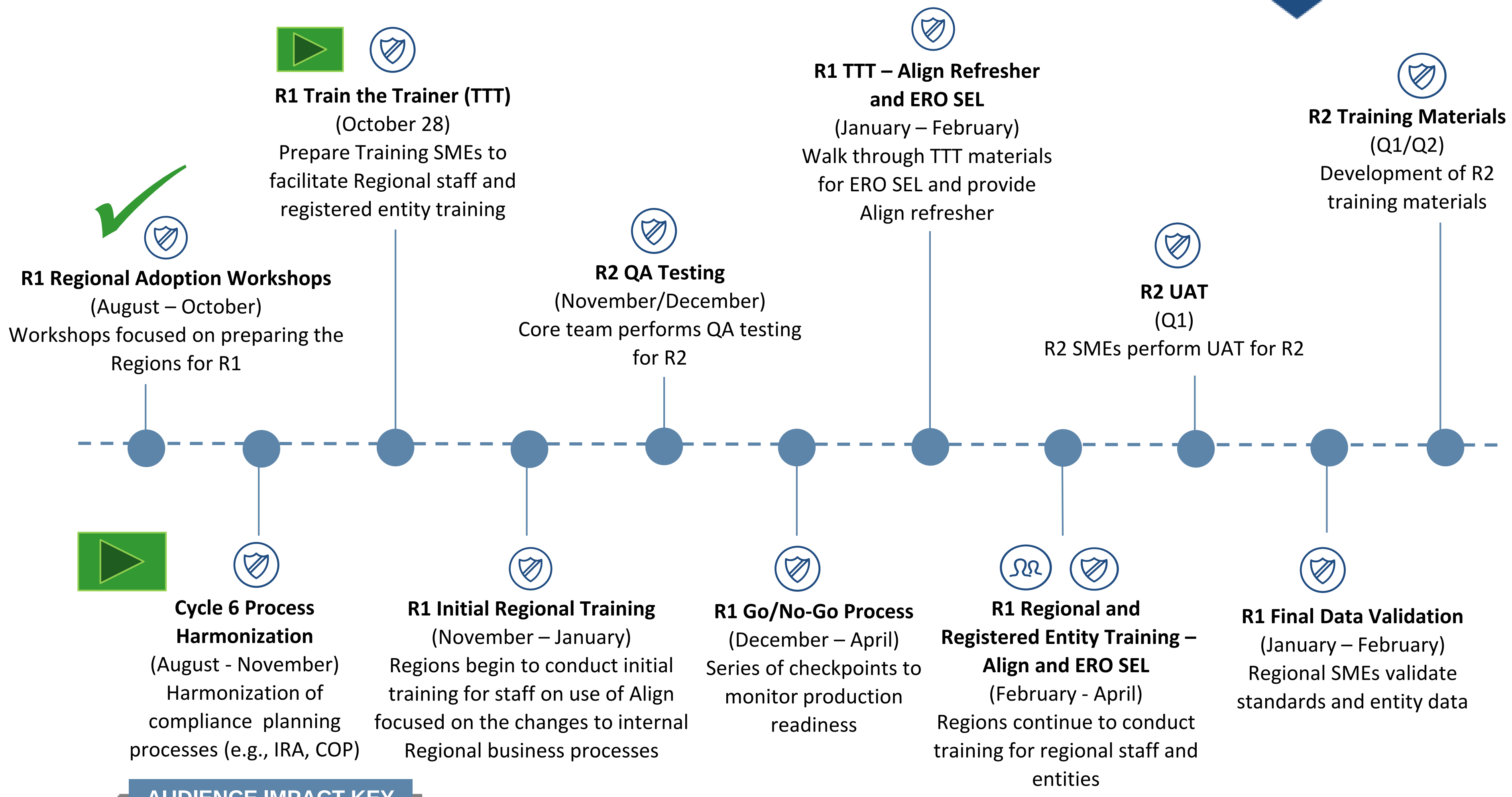
Stan Hoptroff, Vice President, Business Technology
Dee Humphries, Director, Project Management Office
Technology and Security Committee Meeting
November 4, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Major/New Topics
  - Release 1 Timeline Overview and Upcoming Milestones
  - Align Governance Model Update
  - Canada
  - Challenges
  - Change Management
  - How to Stay Informed

Align Timeline and Milestones (As of October 2020)



✓ **R1 Regional Adoption Workshops**
(August – October)
Workshops focused on preparing the Regions for R1

▶ **Cycle 6 Process Harmonization**
(August - November)
Harmonization of compliance planning processes (e.g., IRA, COP)

▶ **R1 Train the Trainer (TTT)**
(October 28)
Prepare Training SMEs to facilitate Regional staff and registered entity training

R1 Initial Regional Training
(November – January)
Regions begin to conduct initial training for staff on use of Align focused on the changes to internal Regional business processes

R2 QA Testing
(November/December)
Core team performs QA testing for R2

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

R1 TTT – Align Refresher and ERO SEL
(January – February)
Walk through TTT materials for ERO SEL and provide Align refresher

R1 Regional and Registered Entity Training – Align and ERO SEL
(February - April)
Regions continue to conduct training for regional staff and entities

R2 UAT
(Q1)
R2 SMEs perform UAT for R2

R1 Final Data Validation
(January – February)
Regional SMEs validate standards and entity data

R2 Training Materials
(Q1/Q2)
Development of R2 training materials

AUDIENCE IMPACT KEY

Registered Entities

ERO Enterprise Staff

▶ *In progress*

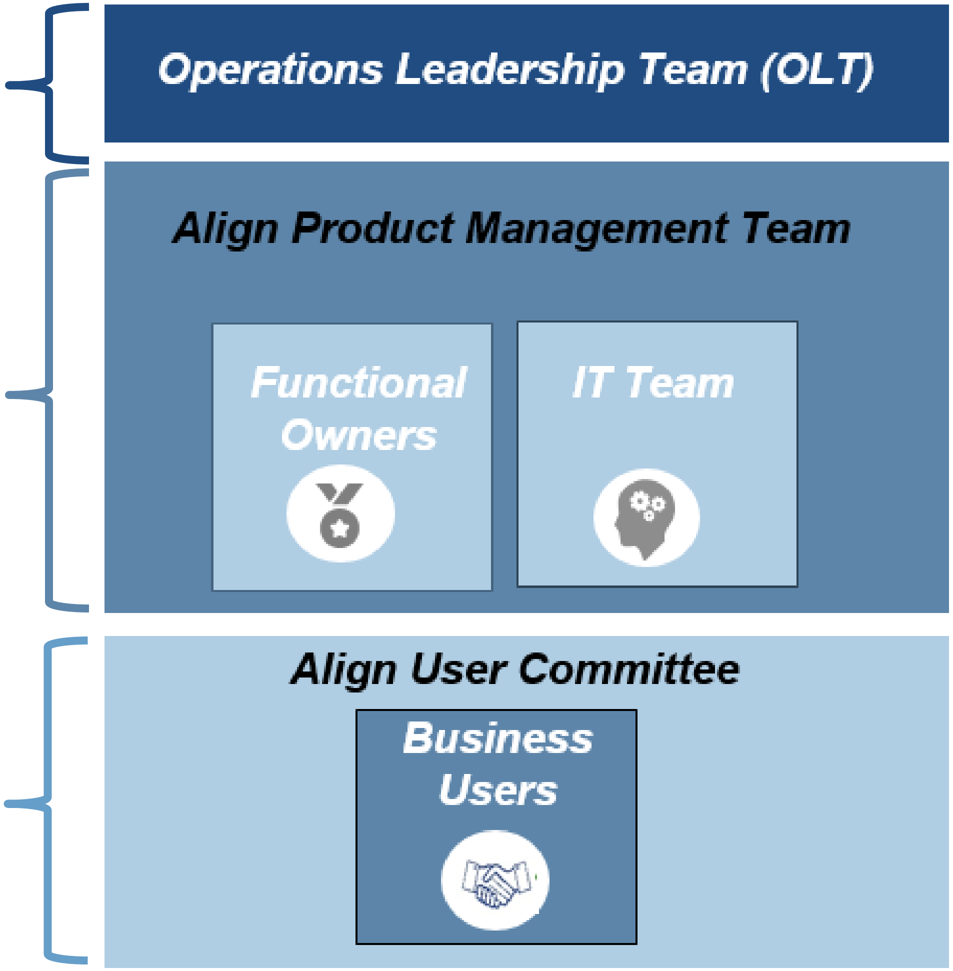
✓ *Complete*

Align Governance

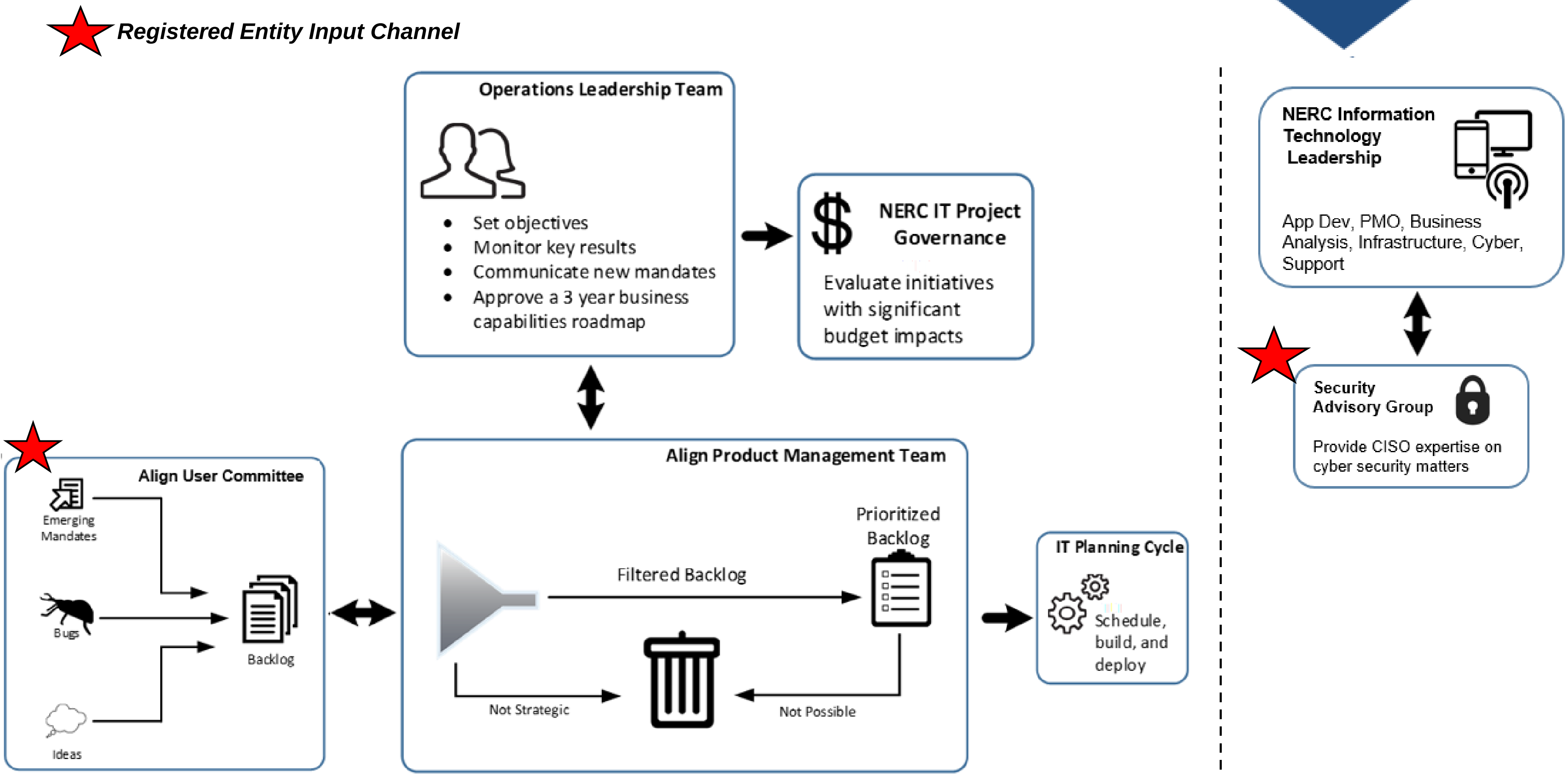
OLT: Provide executive leadership and oversight

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

Interaction Model



★ Registered Entity Input Channel
Operations Leadership Team
Set objectives
Monitor key results
Communicate new mandates
Approve a 3 year business capabilities roadmap
NERC IT Project Governance
Evaluate initiatives with significant budget impacts
NERC Information Technology Leadership
App Dev, PMO, Business Analysis, Infrastructure, Cyber, Support
Security Advisory Group
Provide CISO expertise on cyber security matters
Align User Committee
Emerging Mandates
Bugs
Ideas
Backlog
Align Product Management Team
Filtered Backlog
Prioritized Backlog
Not Strategic
Not Possible
IT Planning Cycle
Schedule, build, and deploy

Transition to this model will take place during 2021

Canadian Provinces and Align Adoption

- In progress to:
  - Determine which provinces will use the U.S. 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

Change Management

- Change Readiness Assessment will take place in November
  - Will measure business readiness for Release 1 go-live
  - Will reach registered entities
  - Will be benchmarked against baseline survey conducted in 2019
- Go-Live Deployment Readiness
  - Will measure technical and operational readiness

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
- NERC News
- Social media

Comments from TVA

1. The ALIGN Project Team has done an INCREDIBLE job!
2. The new ALIGN system looks very impressive, as do the training videos!
3. I am really looking forward to using the new ALIGN system.
4. It will improve the current processes, for the registered entities as well as the Regional Entities and NERC.
5. The training videos provided are excellent! They are short, yet convey a lot of information.
6. The narrator in the training videos does a great job explaining and demonstrating, without making it confusing or too detailed.
7. The new ALIGN system provides a number of enhancements and upgrades, which will make things easier to understand, input, and track.
8. The new ALIGN system screens are much cleaner and easier to follow, along with excellent help text to guide you.

David Abdalla
Senior Program Manager
NERC O&P Compliance

Tennessee Valley Authority

Questions and Answers

Background and Reference Material

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 NERC 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 (PNC) 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 NERC 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

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

ERO Enterprise Secure Evidence Locker Update

Stan Hoptroff, Vice President, Business Technology
Justin Lofquist, IT Director
Technology and Security Committee Meeting
November 4, 2020

RELIABILITY | RESILIENCE | SECURITY

Agenda

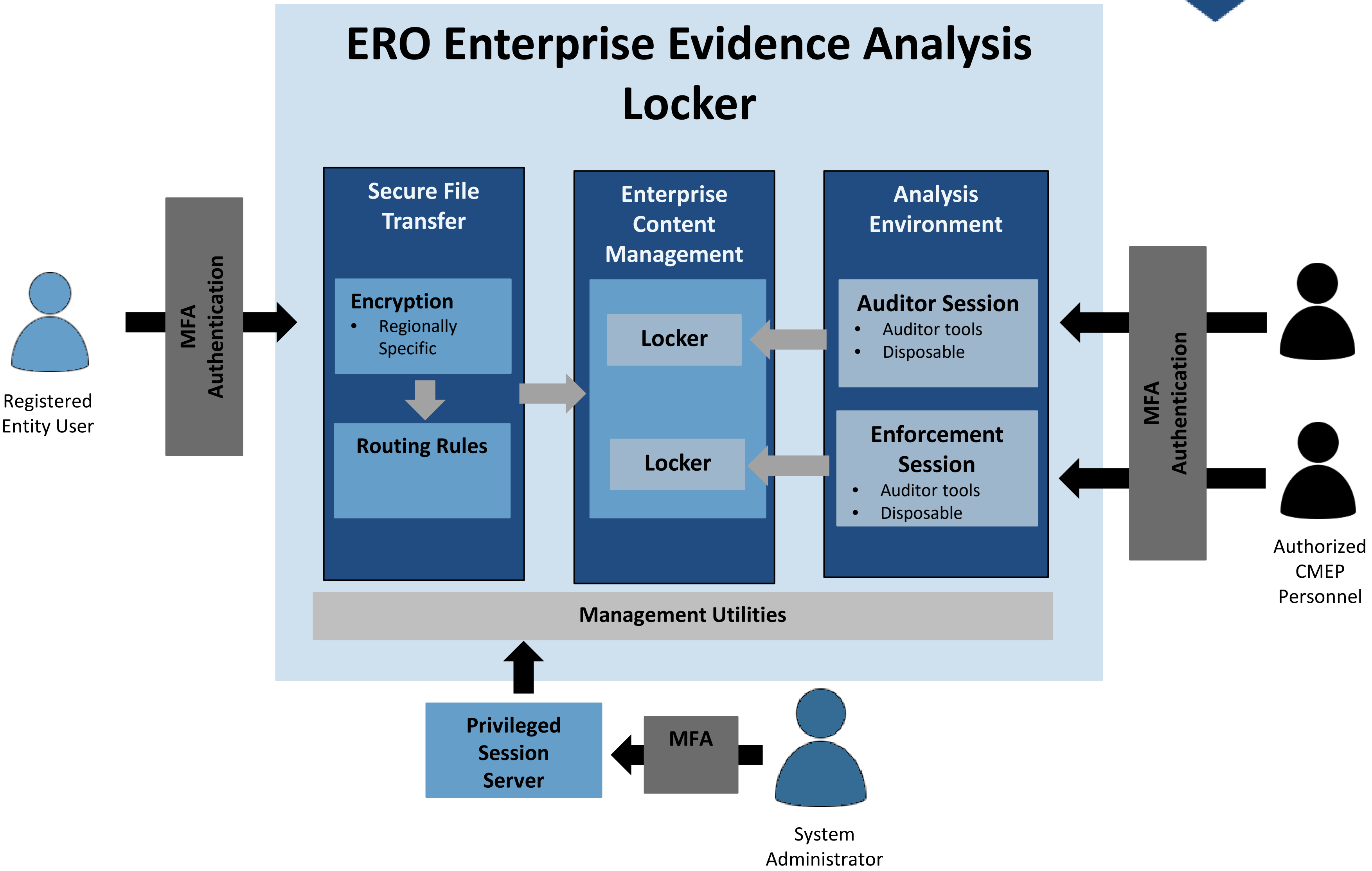
- What is the ERO Enterprise Secure Evidence Locker (ERO SEL)?
- Solution Overview
  - ERO SEL - How Will It Work?
  - National Institute of Standards and Technology (NIST) Standard
  - Security Controls
- Registered Entity Experience Screen Shots
- Regional Entity Experience Screen Shots
- ERO SEL Potential 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 800-171 Standard

- Applicability: Federally-authored for non-governmental agencies handling Controlled Unclassified Information (CUI)
- Contains 110 controls in 14 key areas including:
  - Access Control
  - Physical Protection
  - System and Information Integrity
  - Personnel Security
  - Incident Response
  - Risk Assessment

Evidence Locker - Security

- Proxies for all incoming and out-bound traffic – inspection of all HTTPS traffic
- In-process Virus / malware protection
- Micro-segmentation with Next-Gen firewalls
  - Restricted communications within environment
- Geo-blocking

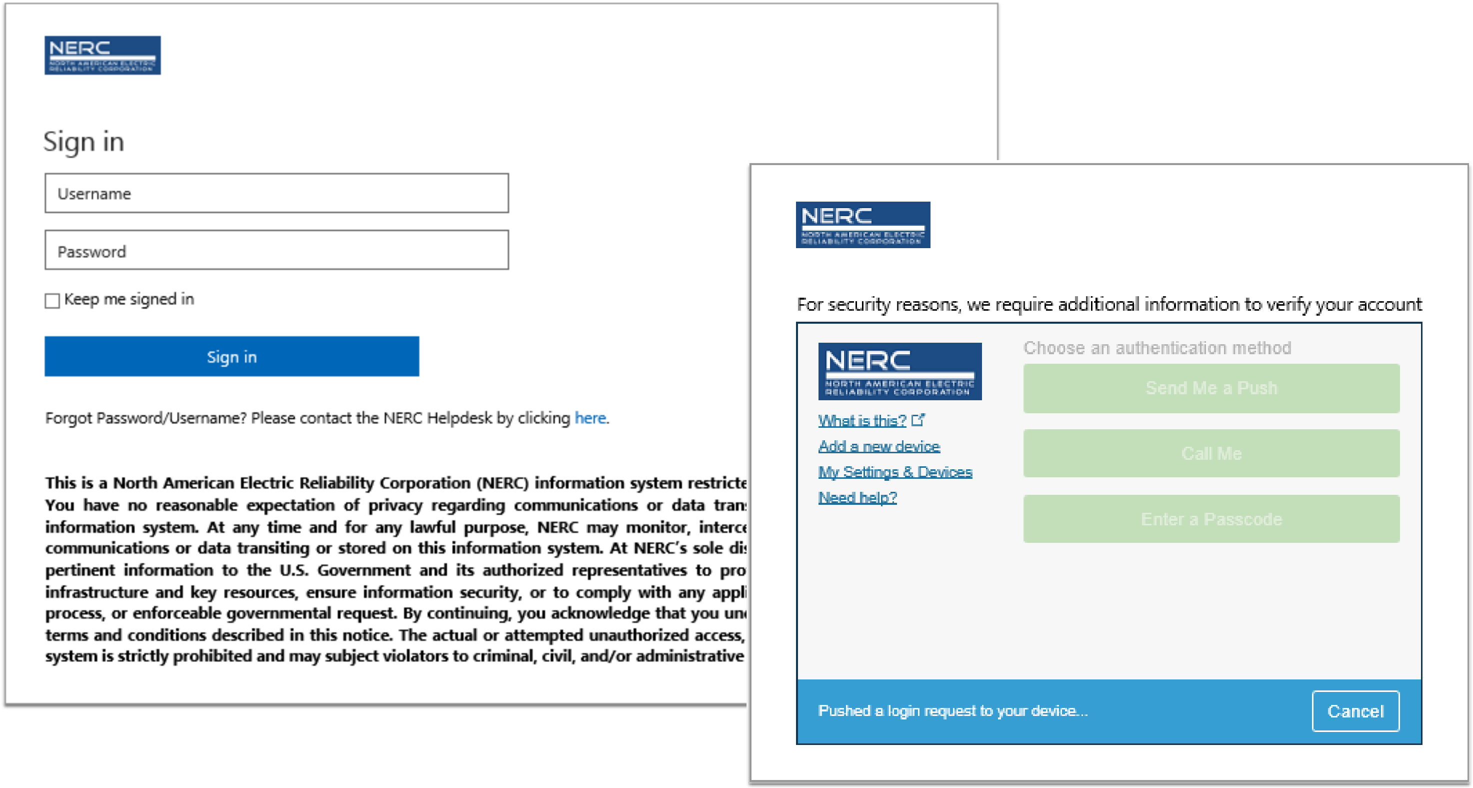
Evidence Locker - Security

- Forensic endpoint monitoring and Network Traffic Analytics
- Enterprise Vulnerability Scanning
- Integrated, key-based authentication (PKI)
  - Encryption of all traffic and data
  - NERC possession and rotation of all encryption keys
- Auditing of all activities and file actions
- Privileged Access Management Service

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)



Sign in

Username

Password

□ Keep me signed in

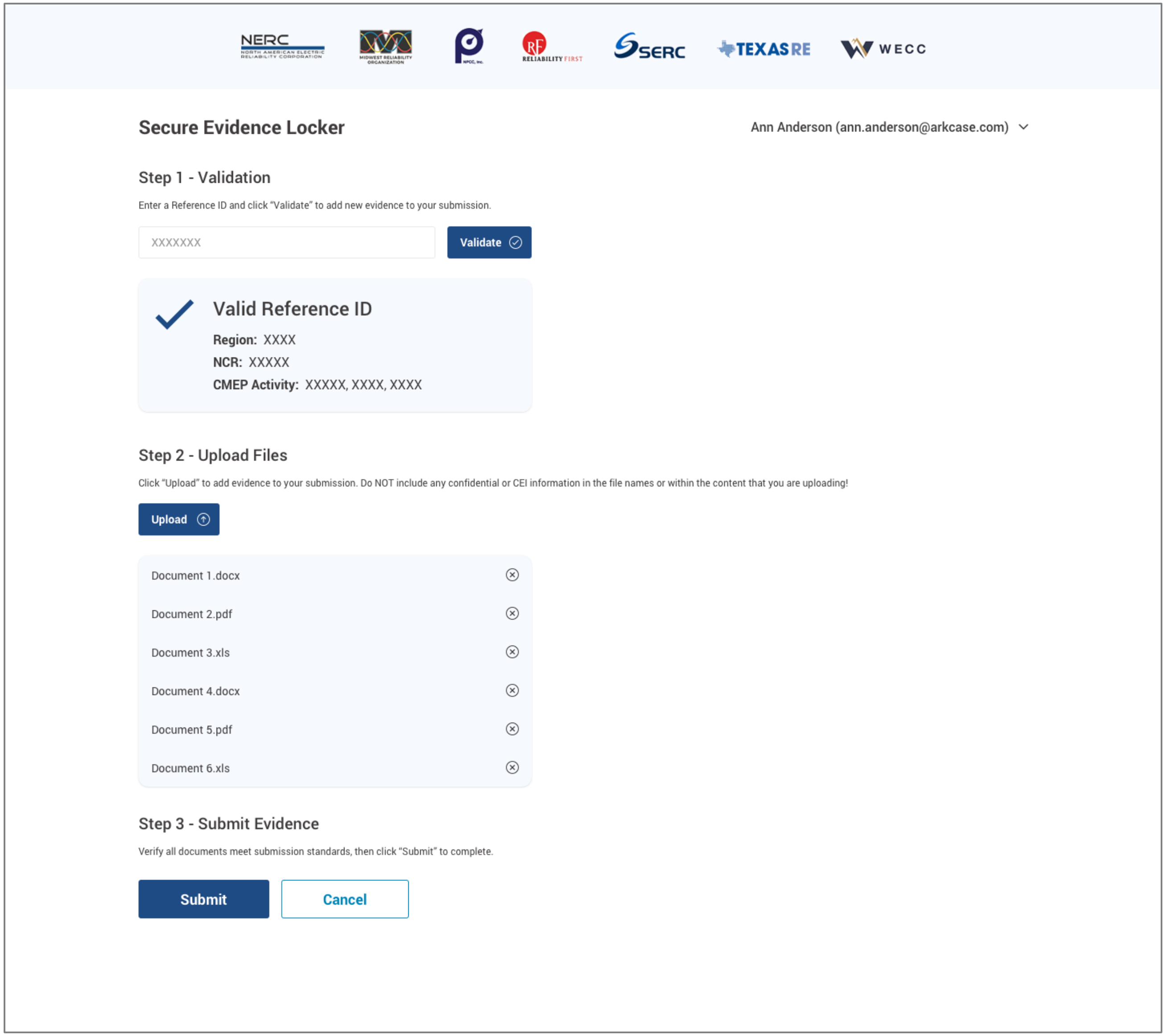
Forgot Password/Username? Please contact the NERC Helpdesk by clicking here.

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 appl
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



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

✓ 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!

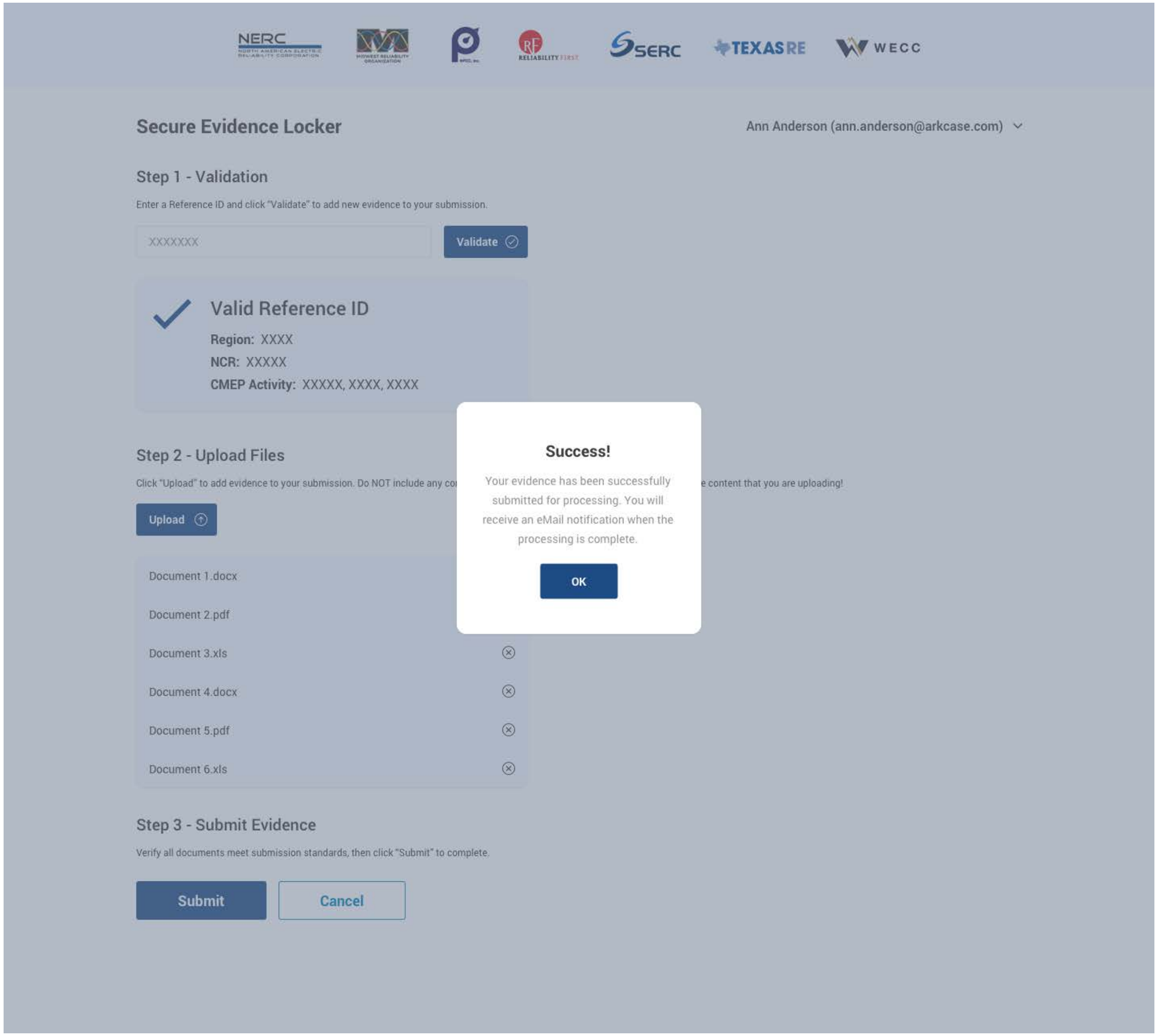
- Document 1.docx ⊗
- Document 2.pdf ⊗
- Document 3.xls ⊗
- Document 4.docx ⊗
- Document 5.pdf ⊗
- Document 6.xls ⊗

Step 3 - Submit Evidence

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

- 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

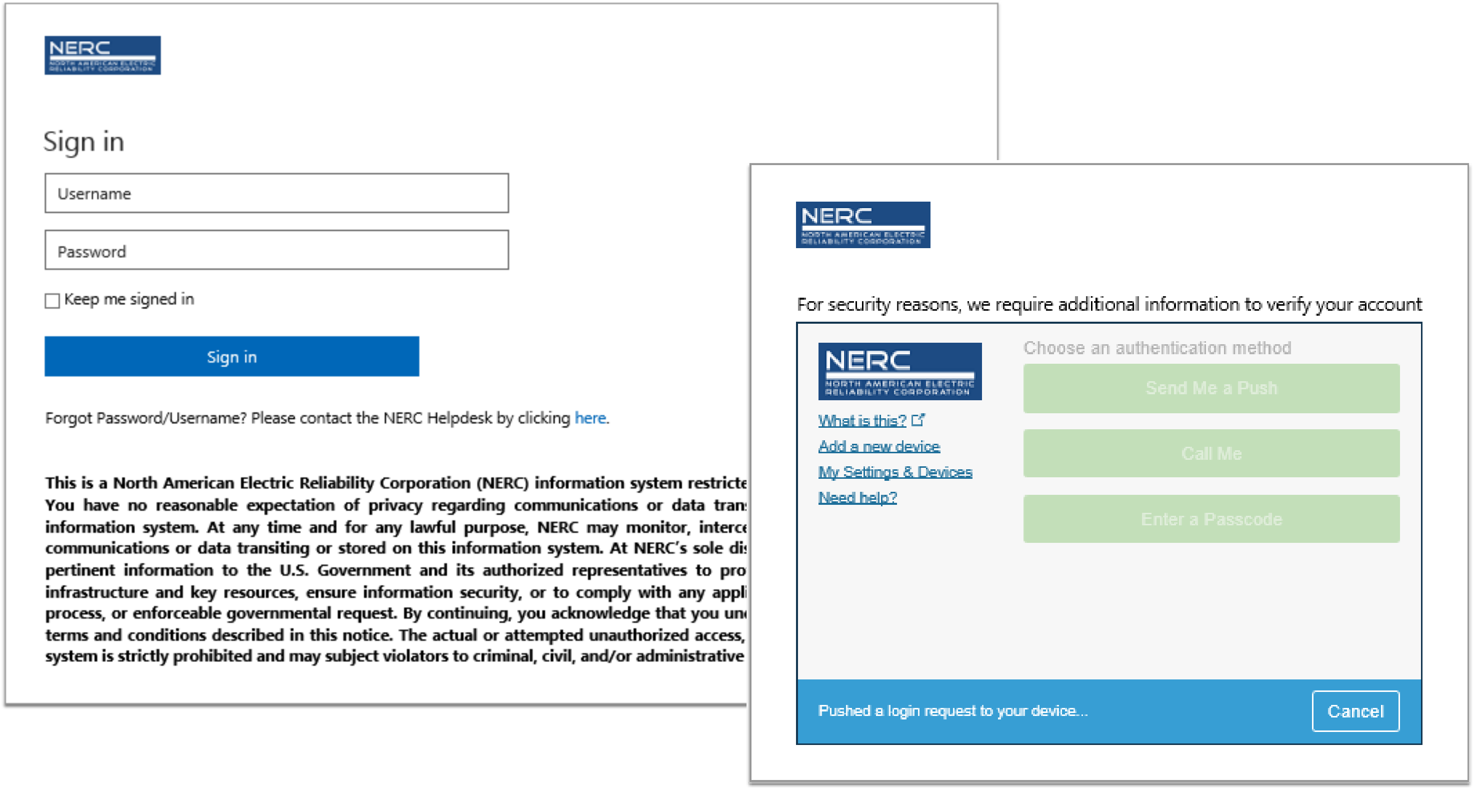
ERO SEL – Regional Entity Experience

- Authenticated through MFA
- No ability to view submitted information (data loss prevention control)
- Ability to request current inventory of evidence per entity

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



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

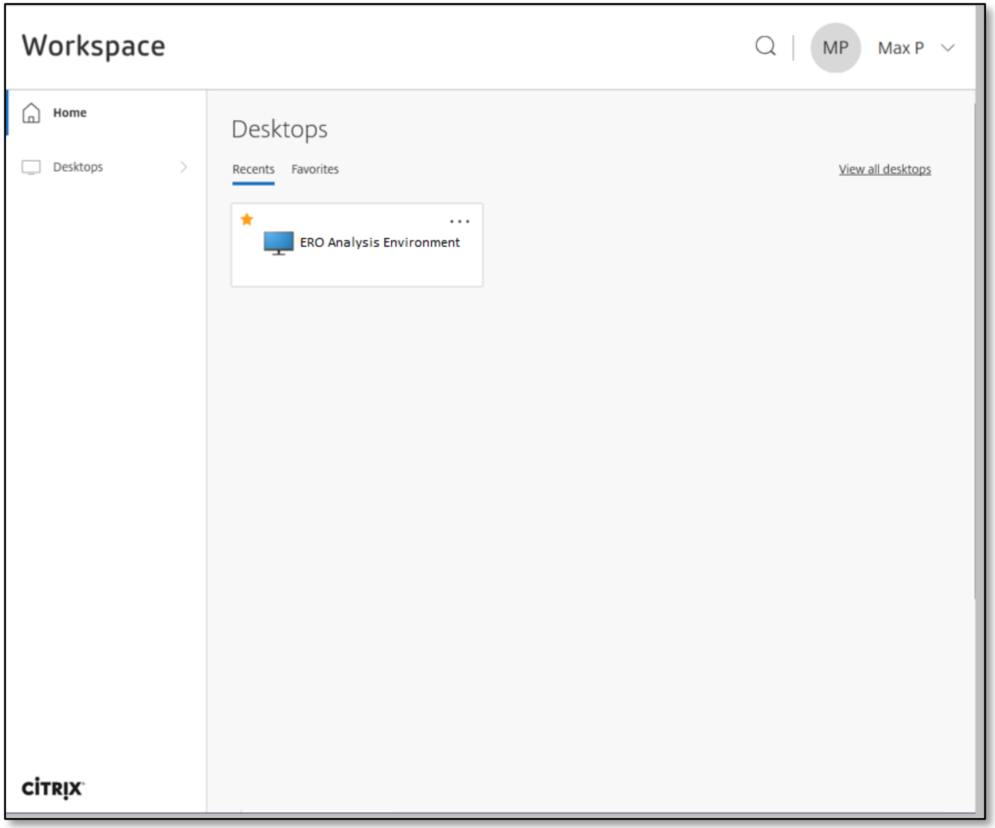
**This is a North American Electric Reliability Corporation (NERC) information system restricte
You have no reasonable expectation of privacy regarding communications or data tran
information system. At any time and for any lawful purpose, NERC may monitor, interce
communications or data transiting or 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...

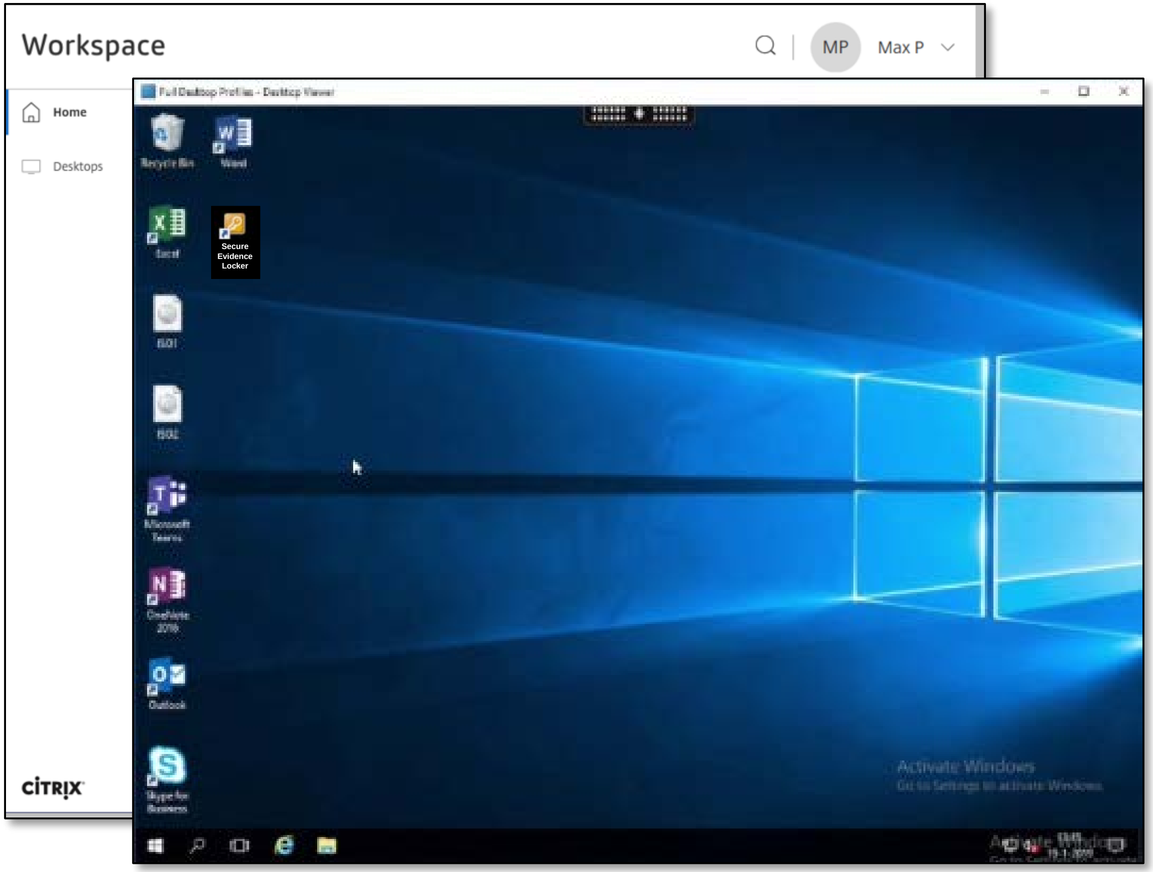
ERO SEL – Regional Entity Experience

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



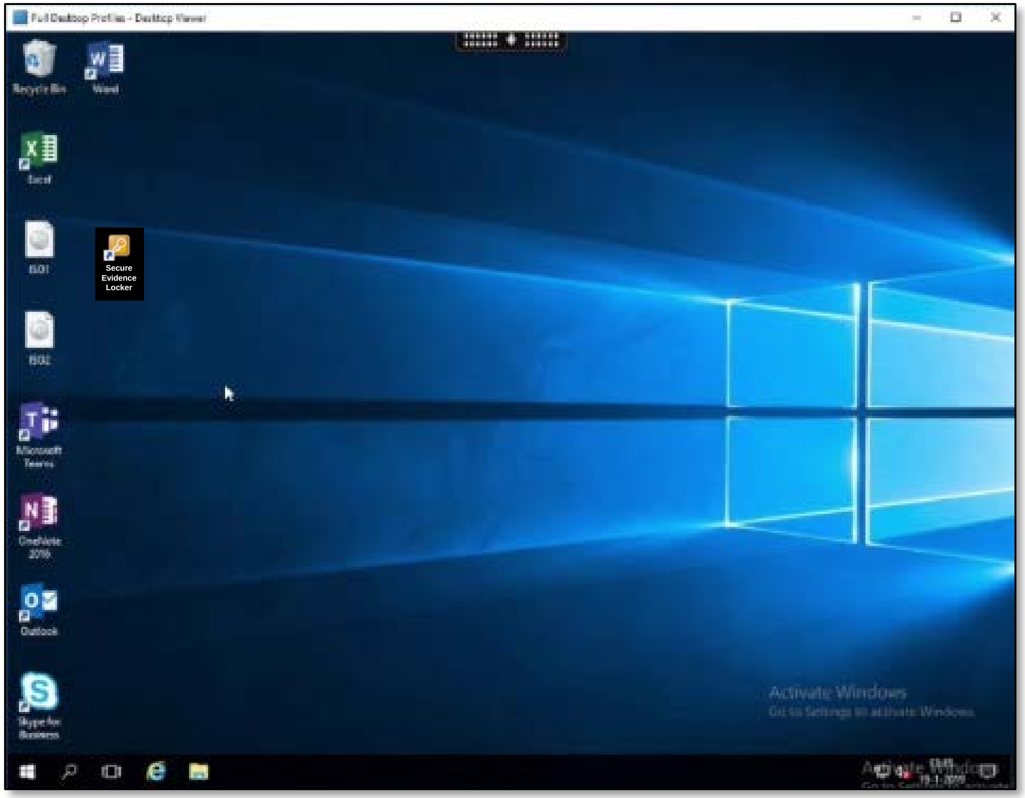
ERO SEL – Regional Entity Experience

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

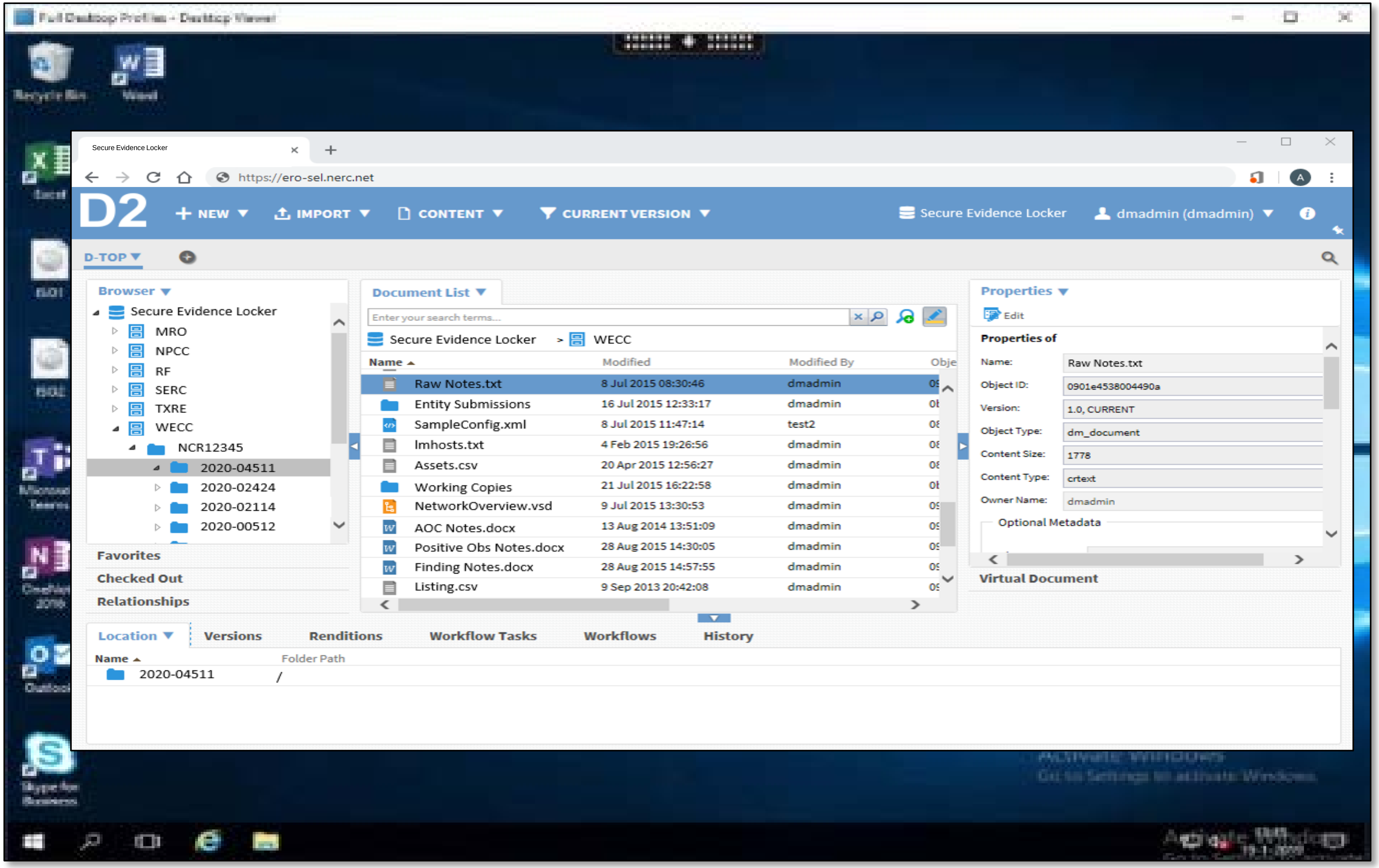


ERO SEL – Regional Entity Experience

- 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



- Secure Evidence Locker
  - MRO
  - NPCC
  - RF
  - SERC
  - TXRE
  - WECC
    - NCR12345
      - 2020-04511
      - 2020-02424
      - 2020-02114
      - 2020-00512

Secure Evidence Locker > WECC

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

Optional Metadata

Name ▲	Folder Path
2020-04511	/

ERO SEL – Regional Entity Experience

- All files are wiped from the Analysis Environment when the user logs out
- No ability to remove evidence from Analysis Environment, e.g., copy / paste (data loss prevention control)
- Access restricted to Regional Corporate networks

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