NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

2019 Business Plan and Budget

Draft 1

May 18, 2018

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

About NERC

Overview

The North American Electric Reliability Corporation (NERC) is a not-for-profit entity organized under the New Jersey Nonprofit Corporation Act. NERC's mission is to assure the effective and efficient reduction of risks to the reliability and security of the Bulk Power System (BPS)[1]. NERC's area of responsibility spans the continental U.S. and portions of Canada and Mexico. Entities under NERC's jurisdiction are the users, owners, and operators of the BPS—a system that serves the needs of over 340 million people, includes installed electricity production capacity of approximately 1,200 gigawatts, operates 475,000 miles of high-voltage transmission (100 kV and above), and is comprised of assets worth more than one trillion dollars.

Electric Reliability Organization

The Federal Energy Regulatory Commission (FERC) certifies and has oversight of NERC as the electric reliability organization (ERO) within the U.S. to establish and enforce NERC Reliability Standards for the U.S. portion of the BPS, pursuant to Section 215 (§215) of the Federal Power Act (FPA). As of June 18, 2007, FERC granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the BPS and made compliance with those standards mandatory and enforceable. Section 215 also requires that the organization certified by FERC as the ERO seek recognition with relevant authorities in Canada and Mexico, and in 2005, the U.S. Department of Energy (DOE) and Canadian federal and provincial governments agreed to bilateral principles for a consistent, continent-wide reliability regulatory framework under a non-governmental institution (the ERO) designed to function on an international basis. To date, eight Canadian provinces[2] and the National Energy Board of Canada have adopted such a framework, and Mexico is in the process of implementing such a framework after a historic restructuring of Mexico's electricity industry and reforms of the country's regulatory framework were enacted in 2013 and 2014. NERC and WECC are working with the Mexican regulator, *Comísion Reguladora de Energía* (CRE) and the Mexican system and market operator, *CENACE*, under a memorandum of understanding (MOU) signed in 2017, to ensure that, as Mexico implements its new authorities, they will be consistent with the framework in Canada and the United States and support continent-wide reliability and security.

Membership and Governance

An 11-member Board, comprised of 10 independent trustees and NERC's president and chief executive officer (CEO) serving as the management trustee, governs NERC. The Board has formed several committees to facilitate oversight of the organization in the areas of finance and audit, governance and human resources, compliance, technology and security, nominations and enterprise-wide risk.

Membership in NERC is open to any person or entity that has an interest in the reliability of the North American BPS. Membership is voluntary and affords participants the opportunity to engage in the governance of the organization through election to the Member Representatives Committee (MRC).[3] More than 600 entities and individuals are members of NERC.

[1] NERC's standards, compliance, and enforcement activities are focused on the Bulk Electric System (BES), which is comprised of certain BPS facilities.

[2] British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, New Brunswick, and Nova Scotia.

[3] The MRC comprises voting representatives elected from the 12 membership sectors. The MRC elects the independent trustees and, along with the Board, votes on amendments to the bylaws. The MRC also provides policy advice and recommendations to the Board on behalf of stakeholders with respect to annual budgets, business plans, and other matters pertinent to the purpose and operation of the organization.

Scope of Oversight

As the international, multijurisdictional ERO in North America, NERC:

- Proposes, supports the development of, monitors compliance with, and enforces mandatory Reliability Standards for the North American BES, subject to regulatory oversight and approvals from FERC in the U.S. and applicable authorities in Canada
- Conducts near-term and long-term reliability assessments of the North American BPS
- Certifies BPS operators as having and maintaining the necessary knowledge and skills to perform their reliability responsibilities
- Maintains situational awareness of events and conditions that may threaten BPS reliability
- Coordinates efforts to improve physical and cyber security for the BPS of North America
- Conducts detailed analyses and investigations of system disturbances and unusual events as well as measuring ongoing system trends to determine root causes, uncovering lessons learned, and issuing relevant findings as advisories, recommendations, guidelines, and essential actions to the industry to mitigate and control risks to reliability
- Identifies and prioritizes risks to reliability and uses a broad toolkit to mitigate and control risks to reliability, including the potential need for new or modified Reliability Standards, improved compliance monitoring and enforcement methods, or other initiatives

Delegated Authorities

In executing its responsibility, NERC delegates certain authorities to regional reliability entities (Regional Entities or the Regions) to perform aspects of the ERO functions described through delegation agreements. FERC has approved delegation agreements between NERC and seven Regional Entities: the Florida Reliability Coordinating Council (FRCC), Midwest Reliability Organization (MRO), Northeast Power Coordinating Council, Inc. (NPCC), ReliabilityFirst (RF), SERC Reliability Corporation (SERC), Texas Reliability Entity, Inc. (Texas RE), and Western Electricity Coordinating Council (WECC). These agreements describe the authorities delegated and responsibilities assigned to the Regional Entities in the U.S. to address, among other things: (1) developing regional Reliability Standards; (2) monitoring compliance with and enforcement of Reliability Standards (both North American-wide and regional); (3) registering owners, operators, and users of the BES and certifying reliability entities (Reliability Coordinators [RCs], Balancing Authorities [BAs], and Transmission Operators [TOPs]); (4) assessing reliability and analyzing performance; (5) training and education; (6) event analysis and reliability improvement; and (7) situational awareness and infrastructure security. NERC expects Regional Entities whose territories and geographic footprints extend into Canadian provinces and Mexico to perform equivalent functions in those jurisdictions.

ERO Enterprise Operating Model

The collective network of leadership, experience, judgment, skills, and technologies shared among NERC and the Regional Entities is referred to as the ERO Enterprise. In 2014, a common operating model, *Improving Coordinated Operations across the ERO Enterprise*,[4] was developed to define how NERC and the Regional Entities achieve excellence in the oversight and execution of statutory functions by collaborating to mitigate reliability risks. The model also defines the division of the roles and responsibilities for NERC and the Regional Entities to efficiently and effectively execute services performed as the collective ERO Enterprise.

[4] Improving Coordinated Operations Across the ERO Enterprise

NERC has unique responsibilities within the ERO Enterprise to design the oversight of program areas, develop operational oversight and leadership, set qualifications and expectations for the performance of delegated activities, and assess, train, and give feedback to corresponding Regional Entity programs. Implementation of the operating model progressed with NERC's finalization of documented oversight plans for all statutory program areas for which the Regional Entities' have delegated activities. Further, NERC and the Regional Entities have deepened their coordination activities to identify, prioritize, and address risks to reliability. NERC also reviews and provides input to the annual Regional Entity business plans and budgets (BP&Bs), including but not limited to review of resource allocations, staffing capacity assessments, and program performance assessments. NERC input and review occurs before Regional Entity board approval.

Similarly, the Regional Entities have a mirrored set of responsibilities that include being responsive to the design of the operational model, providing input into the overall development of each ERO program area, providing training and development to meet ERO qualifications, being receptive to feedback from the ERO, and making responsive adjustments. Regional Entities also have an obligation to meet professional standards of independence and objectivity and provide the best available expertise for addressing risks.

With due recognition and awareness of the distinction between individual roles, responsibilities, and corporate status, NERC and the Regional Entities are continually refining their individual and collective operating and governance practices in support of an agreed-upon set of strategic and operational goals and objectives that are designed to ensure the ERO fulfills its statutory obligations.

Statutory and Regulatory Background

NERC's authority as the ERO in the U.S. is based on §215 of the FPA, as added by the Energy Policy Act of 2005,[5] and FERC's regulations and orders issued pursuant to §215. In Canada, NERC's authorities are established by the memoranda of understanding and regulations previously mentioned.

Funding

Section 215 of the FPA and FERC's regulations specify procedures for NERC's funding in the U.S. NERC's annual BP&B is subject to FERC approval in the U.S and, once approved, NERC's annual funding is provided primarily through assessments to load-serving entities. These assessments are allocated on a net-energy-for-load (NEL) basis. Equivalent funding mechanisms are provided in Canada, subject to the specific laws and regulations of each province.

The Regional Entities' funding requirements are addressed separately in their respective BP&Bs, which must be reviewed and approved by NERC and FERC. The U.S. assessments for the Regional Entity budgets are included in the overall NERC assessments to load-serving entities.

[5] This was codified in §215 of the FPA, 16 United States C. 824o.

Introduction and Executive Summary

TOTAL RESOURCES (in whole dollars)	2019 Budget	U.S.	Canada	Mexico
Statutory FTEs	204.92			
Non-statutory FTEs	-			
Total FTEs	**204.92**			
Statutory Expenses	$ 78,717,528			
Non-Statutory Expenses	$ -			
Total Expenses	**$ 78,717,528**			
Statutory Inc (Dec) in Fixed Assets	$ 1,331,978			
Non-Statutory Inc (Dec) in Fixed Assets	$ -			
Total Inc (Dec) in Fixed Assets	**$ 1,331,978**			
Statutory Funding of Reserves	$ 133,977			
Non-Statutory Funding of Reserves	$ -			
Total Working Capital Requirement	**$ 133,977**			
Net Proceeds from Financing Activities	**$ (1,067,980)**			
Total Statutory Funding Requirement	$ 79,115,503			
Total Non-Statutory Funding Requirement	$ -			
Total Funding Requirement	**$ 79,115,503**			
	TOTAL	**US**	**CANADA**	**MEXICO**
Statutory Funding Assessments	**$ 69,449,054**	**TBD**	**TBD**	**TBD**
Non-Statutory Fees	**$ -**	**$ -**	**$ -**	**$ -**
NEL	**-**	**TBD**	**TBD**	**TBD**
NEL%	**-**	**TBD**	**TBD**	**TBD**

Strategic and Operational Planning

The ERO Enterprise's strategic and operational planning process is informed by ongoing activities to identify (1) BPS reliability risks, particularly informed by the Reliability Issues Steering Committee's (RISC's) biennial reliability leadership summit and *ERO Reliability Risk Priorities Report*[6] (RISC report), and (2) opportunities to improve ERO Enterprise effectiveness and efficiency. The transparent and collaborative process includes input from stakeholders[7], the Board, and Regional Entity boards. These inputs are used by ERO Enterprise leadership to inform the following strategic and operational planning components:

- **ERO Enterprise Long-Term Strategy**[8] – The long-term strategy discusses key challenges and strategic focus areas for the ERO Enterprise over the next five to seven years. The long-term strategy is reviewed on a periodic basis to identify any needed adjustments.
- **ERO Enterprise Operating Plan**[9] – Guided by the long-term strategy, the operating plan identifies the ERO Enterprise's vision, mission, core principals, and goals, and provides a list of key contributing activities[10] by the combined ERO Enterprise, NERC, and the Regional Entities as applicable to inform a rolling three-year operational planning horizon. The operating plan is reviewed biennially[11] and updated as needed.
- **ERO Enterprise BP&Bs** – BP&Bs set the specific annual activities, resources, and resource allocation in support of the goals and objectives in the operating plan. BP&Bs are prepared, reviewed, and approved annually for NERC and each of the Regional Entities.
- **ERO Enterprise Metrics**[12] – The metrics include measures, thresholds, and targets to provide indicators of BPS reliability and security as well as ERO Enterprise effectiveness and efficiency. The metrics are reviewed annually and updated as needed to ensure they meaningfully inform near and long-term priorities.[13]

Evolving Reliability Risks

Over the past several years, NERC has transformed its activities towards being more risk-based, ensuring that the right activities are focused on the most pertinent risks to the reliable operation of the BPS. The RISC is an advisory committee to the Board, providing key insights, priorities, and high-level leadership for issues of strategic importance to BPS reliability. The latest RISC report, which was accepted by the Board on February 8, 2018, presents the results of its continued work to define and prioritize risks and to offer recommendations to the Board to inform the development of NERC's risk strategy. The RISC report recommendations are considered as the operating plan's goals and contributing activities are updated for the coming years. In the latest report, the RISC recommended a high level of focus and priority on the following areas that have been identified as having a higher likelihood of BPS-wide occurrence and higher impact to BPS reliability.

[6] ERO Reliability Risk Priorities Report (Board Accepted February 8, 2018)

[7] This includes input from the RISC, MRC, NERC standing and technical committees, trade associations and industry forums, as well as public comment periods.

[8] ERO Enterprise Long-Term Strategy (Board Approved November 9, 2017)

[9] ERO Enterprise Operating Plan (Board Approved November 9, 2017)

[10] Activities that are recommendations from the RISC report are labeled accordingly.

[11] The operating plan is reviewed same year the RISC reviews and updates its report.

[12] 2018 ERO Enterprise Metrics (Board Approved November 9, 2017)

[13] Each ERO Enterprise entity establishes additional metrics to support performance-based compensation programs. These metrics typically measure achievement of specific objectives, tasks, and activities on a departmental or company-wide basis for the operating year.

Cybersecurity Vulnerabilities
Cyber threats are becoming more sophisticated and increasing in number. Exploitation of cybersecurity vulnerabilities can cause loss of control or damage to BPS-related voice communications, data, monitoring, protection and control systems, or tools. A cyber-attack can result in equipment damage, degradation of reliable operations, uncontrolled cascading of the BPS, and loss of load. Further, cybersecurity vulnerabilities can come from several sources, both internal and external, and in some instances the utility may have its cybersecurity fully tested.

Changing Resource Mix
The rapid rate at which fuel costs, subsidies, and federal, state, and provincial policies are affecting the resource mix are creating a new paradigm in which planners, balancing authorities, and system operators are reacting to resource additions and retirements. Further, the integration of new technologies and distributed energy resources are affecting the ability of operators to see and control resources within their area.

BPS Planning
BPS planning is a risk closely tied to the changing resource mix because planners currently lack the ability to update or create system models and scenarios of potential future states to identify system needs based on the dynamic nature of the system. This changing system makes it increasingly difficult to evaluate BPS stability, including inertia and frequency response, voltage support (adequate dynamic and static reactive compensation), and ramping constraints.

Resource Adequacy
Changes in the generation resource mix and new technologies are altering the operational characteristics of the grid and will challenge system planners and operators to maintain reliability in real time. Failure to take into account these changing characteristics and capabilities can lead to insufficient capacity and essential reliability services to meet customer demands.

ERO Enterprise Goals

As part of the *ERO Enterprise Operating Plan* discussed above, the ERO Enterprise has six goals enabling the ERO Enterprise to successfully carry out its mission. A description of each goal is provided below, followed by additional information about the allocation of NERC's and the full ERO Enterprise's resources toward achievement of each goal.

Goal 1: Risk-Responsive Reliability Standards
Reliability Standards establish threshold requirements for assuring the BES is planned, operated, and maintained to minimize risks of cascading failures, avoid damage to major equipment, or limit interruptions of the BPS. Reliability Standards are clear, timely, effective in mitigating risks to reliability, and consider cost-effectiveness/impact.

Goal 2: Objective, Risk-Informed Compliance Monitoring, Mitigation, Enforcement, and Entity Registration
The ERO Enterprise is a strong enforcement authority that is objective, fair, and promotes a culture of reliability excellence through risk-informed compliance monitoring, mitigation, enforcement, and registration.

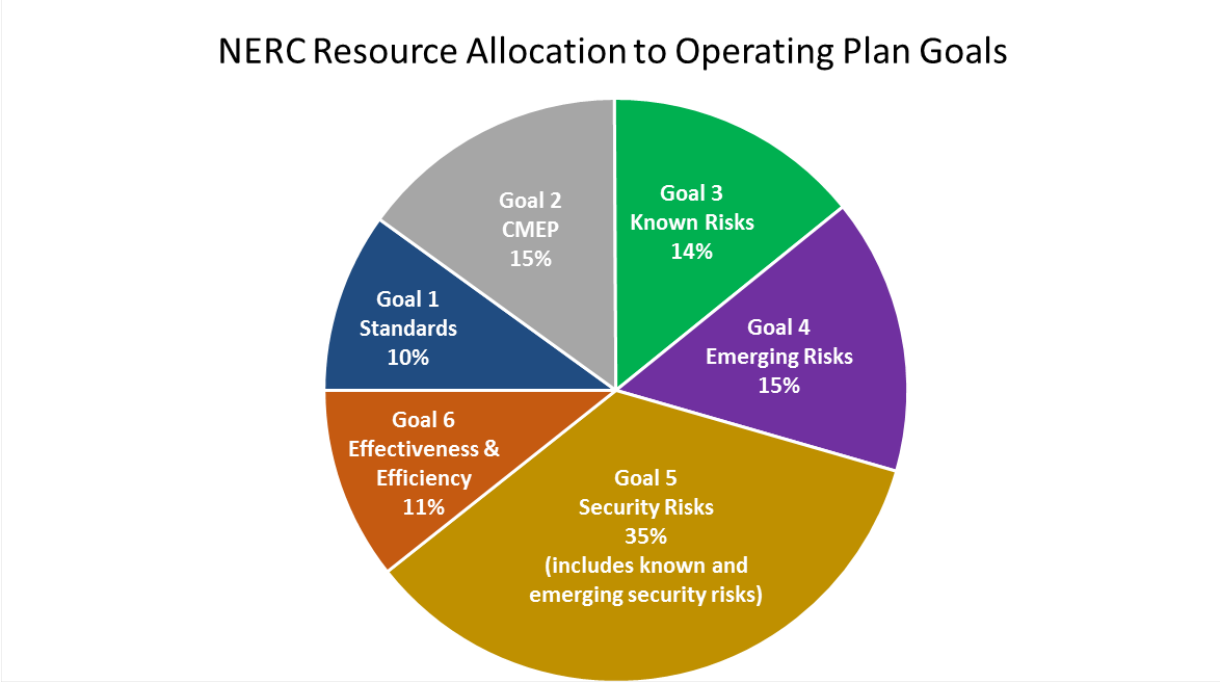
Goal 3: Reduction of Known Reliability Risks
The ERO Enterprise recognizes significant known risks to reliability, assures those risks are reduced, and promotes a culture of reliability excellence.

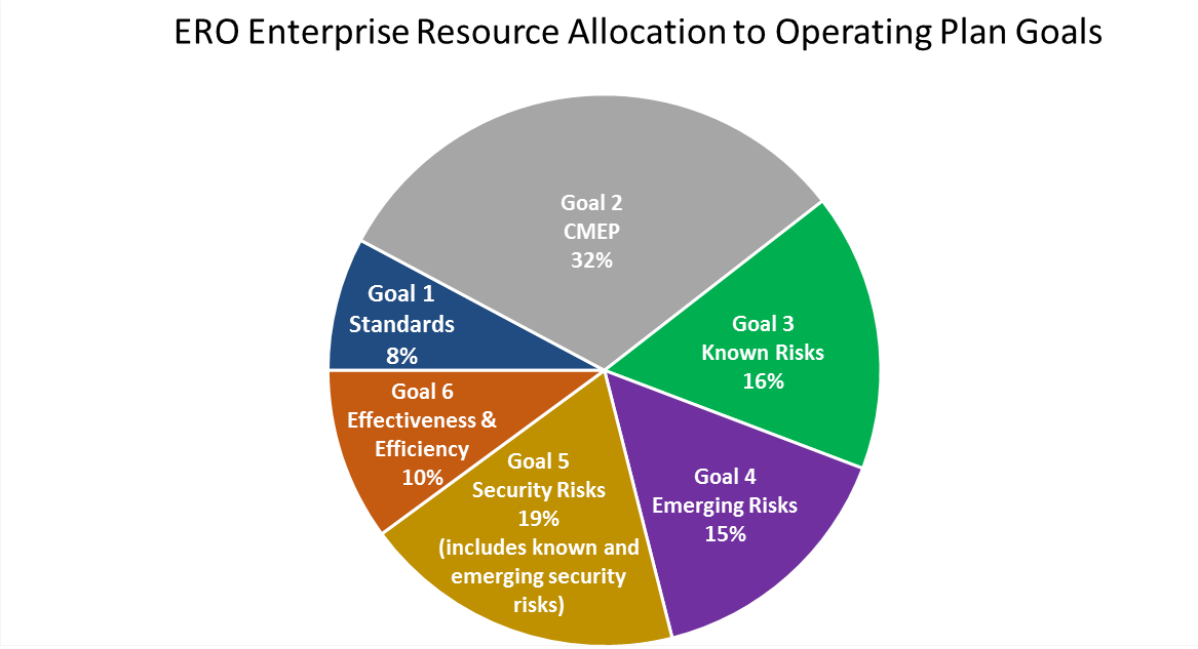
Goal 4: Identification and Assessment of Emerging Reliability
The ERO Enterprise identifies, objectively assesses, and prioritizes emerging risks to reliability to inform stakeholders and enable effective actions to reduce these risks to reliability.

Goal 5: Identification and Reduction of Cyber and Physical Security Risks
The ERO Enterprise identifies and evaluates cyber and physical security risks to the BPS and assures those risks are reduced through active stakeholder engagement and information sharing of current threats and vulnerabilities, security workshops, and development of good industry practice guides. The ERO Enterprise supports the Electricity Information Sharing and Analysis Center (E-ISAC), the Cybersecurity Risk Information Sharing Program (CRISP), technical protective programs, and physical and cybersecurity preparedness exercises, and engages with government partners to de-classify sensitive security information needed to protect BPS devices and assets. The ERO Enterprise works with stakeholders to develop and share information to foster BPS resiliency in connection with both traditional and emerging risks.

Goal 6: Effective and Efficient Operations
The ERO Enterprise embraces transparency, collaboration, consistency, quality, efficiency, and timeliness of results and operates as a coordinated and collaborative enterprise.

Allocation of NERC Resources to ERO Enterprise Goals and Risk Priorities
The charts below provide an overview of the allocation of both NERC and the ERO Enterprise's 2019 resources associated with each goal in the *ERO Enterprise Operating Plan* and the related contributing activities discussed above. Using surveys, funding sources, and FTEs as a guide, the charts reflect the relative amount of total resources (people and dollars) focused on supporting each of the six goals noted above. Since many departments work on multiple activities that further multiple goals, forecasting all activities supporting each goal is not precise. However, these charts provide a general picture regarding how resources are allocated.





Ongoing Focus on Effectiveness and Efficiency

NERC and the Regional Entities continue to collaborate to improve effectiveness and efficiency, evaluate resources, and leverage combined skillsets to improve ERO Enterprise activities and control costs. This collaboration and resulting efficiencies can be found in a number of areas, including but not limited to:

- **ERO Enterprise IT investments** – NERC and the Regional Entities, under the oversight of the Board Technology and Security Committee (TSC), have developed a long-term ERO Enterprise IT program resulting in a number of enterprise tools to enhance operations, improve efficiency, and reduce costs at the NERC, regional, and registered entity levels. For example, these tools will facilitate efficiency of data submittals, consistency in compliance resources, and overall reliability through information sharing related to event analysis, misoperations, and situational awareness.
- **Enforcement** – NERC has worked closely with Regional Entities to streamline enforcement processes, and therefore required resources, in connection with the development of more efficient and risk-based enforcement mechanisms.
- **Standards** – As standards development has matured, NERC management has reallocated Standards staff towards more critical activities like cyber security and analytical capabilities.
- **Forums** – As further described in the quarterly forum reports to the Board, NERC and the Regional Entities continue to leverage the transmission and generation forums to jointly address risks to reliability to mitigate their impacts on the reliable operation of the BES.
- **Industry** – The ERO Enterprise continues to collaborate with and rely on industry resources and expertise through the various standing and technical committees, working groups, and task forces that are critical to both identifying and supporting key initiatives and priorities.

Additional information on long-term and ongoing effectiveness and efficiency goals can be found in Focus Area 2 of the *ERO Enterprise Long-Term Strategy*, Goal 6 of the draft *ERO Enterprise Operating Plan*, and Metric 7d of the *2018 ERO Enterprise Metrics.* Current efforts in support of these goals are detailed in a draft framework for improving ERO Enterprise effectiveness and efficiency that was presented and discussed at the May 9 MRC meeting. [14]

[14] MRC Agenda Package – May 9, 2018 (see agenda item 8)

2019 Key Business Planning Assumptions

NERC and the Regional Entities use the goals and contributing activities in the *ERO Enterprise Operating Plan* as a guide to support the development of their respective BP&Bs. NERC and the Regional Entities use this planning information to evaluate their projected workloads and determine resource levels and allocation required to complete necessary tasks and meet their statutory obligations.

Application of Section 215 Criteria

In its order approving NERC's *2013 Business Plan and Budget*, FERC required NERC to establish criteria for determining whether its proposed activities are eligible for funding under §215. In an order dated April 19, 2013, FERC approved NERC's proposed criteria, with certain modifications.[15] *Exhibit A – Application of NERC Section 215 Criteria* summarizes the major activities NERC proposes to undertake in 2019 and the approved §215 criteria applicable to such activities.

Overview of 2019 Budget and Funding Requirements

NERC's 2019 combined expense and fixed asset (capital) budget is approximately $80.0M, which represents an increase of approximately $6.9M (9.5%) from the 2018 budget. Total expenses are increasing approximately $7.9M (11.1%) over 2018. The total fixed asset (capital) budget, excluding depreciation,[16] is approximately $4.8M, an increase of $904k (23.3%) from 2018. Approximately $9.0M (11.2%) of NERC's 2019 budget is related to CRISP, with the majority of the CRISP budget funded by participating utilities, with a small portion funded through assessments.

NERC's proposed 2019 assessment is approximately $69.5M, which represents an increase of $6.5M (10.3%) from 2018. Factors contributing to the difference between the proposed budget increase and the proposed assessment increase include debt (capital financing) assumptions and changes from 2018 to 2019 in other funding from CRISP, workshop fees, etc. In addition, 2018 funding included a $600k transfer from the Assessment Stabilization Reserve. The 2019 assessment increase does not reflect a proposed release of funds from the Assessment Stabilization Reserve, which is discussed below.

In order to stabilize assessments and align budget and assessment increases more closely, NERC has undertaken a multi-year strategy to manage assessment increases. NERC's policy *Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards*[17] and NERC Rules of Procedure (ROP) §1107.2 specify that penalties received during the period July 1 through the following June 30 are to be used in the subsequent budget period to offset U.S. assessment billings. However, ROP §1107.4 provides for exceptions or alternatives to this treatment if approved by FERC. In February 2015, the Board approved an amendment to the company's *Working Capital and Operating Reserve Policy*.[18] Among the approved changes was the creation of an Assessment Stabilization Reserve.[19] This reserve was established to implement the strategic goal of more closely

[15] North American Electric Reliability Corporation, Order on Compliance, 143 FERC ¶ 61,052 (2013).

[16] NERC and the Regional Entities budget depreciation as an operating expense with an equal and offsetting credit against budgeted Fixed Asset (capital) additions. As a result, the budgets do not include depreciation in the funding requirements.

[17] Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standards, December 8, 2008 and as amended August 15, 2013.

[18] NERC's Working Capital and Operating Reserve Policy. NERC filed a petition with FERC on March 6, 2015 for approval of this policy; FERC conditionally approved the revised policy in an order issued June 18, 2015, in Docket No. RR15-8-000. *North American Electric Reliability Corporation, Order Conditionally Accepting Revisions to Working Capital and Operating Reserve Policy*, 151 FERC ¶ 61,225 (2015). On August 14, 2015, NERC submitted a compliance filing to the June 18, 2015 order with a modification to the policy, which FERC accepted by letter order dated September 18, 2015 (Docket No. RR15-8-001).

[19] In accordance with the approved *Working Capital and Operating Reserve Policy*, the Assessment Stabilization Reserve may be funded with penalty funds and surplus operating reserves. The actual amount of the contribution, as well as releases from the

aligning annual budget and U.S. assessment increases and to better manage year-to-year assessment increases. The eventual goal is to narrow the gap between annual percentage changes in NERC's budget and annual percentage changes in assessments that result from year-to-year variations in penalty collections.

Subject to Board and FERC approval, NERC will deposit any penalties collected during the period July 1, 2017–June 30, 2018, into the Assessment Stabilization Reserve. NERC and the Board are also considering a release of $564k from the Assessment Stabilization Reserve to reduce 2019 assessments, resulting in a matching 2019 budget and assessment increase of 9.5%. The allocation of assessments to Canadian entities will depend on the final determination and allocation of certain compliance and enforcement costs to Canadian entities pursuant to NERC's policy on the allocation of compliance costs.[20]

The following table provides a high-level year-over-year comparison of the major categories of expenses, total budget, and full-time equivalents (FTEs).

Statement of Activities and Fixed Assets Expenditures 2018 and 2019 Budgets

STATUTORY

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)	% Over (Under)
Funding						
ERO Funding						
NERC Assessments	$ 62,936,968	$ 62,936,968	$ -	$ 69,449,054	$ 6,512,086	10.3%
Assessment Stabilization Reserve - Penalties	600,000	600,000	-	-	(600,000)	
Third-Party Funding (CRISP)	7,324,253	7,225,735	(98,518)	7,456,449	132,196	
Testing Fees	1,790,000	1,728,075	(61,926)	1,790,000	-	
Services & Software	50,000	50,000	-	40,000	(10,000)	
Workshops	185,000	185,000	-	195,000	10,000	
Interest	95,000	292,439	197,438	185,000	90,000	
Miscellaneous	-	-	-	-	-	
Total Funding	**$ 72,981,221**	**$ 73,018,216**	**$ 36,995**	**$ 79,115,503**	**$ 6,134,282**	**8.4%**
Expenses						
Personnel Expenses	$ 40,969,105	$ 41,450,947	$ 481,842	$ 44,150,446	$ 3,181,341	7.8%
Meeting Expenses	3,395,100	3,331,353	(63,747)	3,395,400	300	0.0%
Operating Expenses	26,352,371	26,600,975	248,604	30,957,511	4,605,139	17.5%
Other Non-Operating	138,878	138,878	-	214,171	75,293	54.2%
Total Expenses	**$ 70,855,455**	**$ 71,522,153**	**$ 666,699**	**$ 78,717,528**	**$ 7,862,074**	**11.1%**
Fixed Assets						
Depreciation	$ (1,594,299)	$ (1,594,299)	$ -	$ (3,446,022)	$ (1,851,724)	
Computer & Software CapEx	2,549,000	2,549,000	-	3,488,000	939,000	
Equipment CapEx	1,175,000	1,175,000	-	890,000	(285,000)	
Leasehold Improvements	150,000	150,000	-	400,000	250,000	
Inc(Dec) in Fixed Assets	**$ 2,279,701**	**$ 2,279,701**	**$ -**	**$ 1,331,978**	**$ (947,724)**	**-41.6%**
Total Budget	**$ 73,135,156**	**$ 73,801,855**	**$ 666,699**	**$ 80,049,506**	**$ 6,914,350**	**9.5%**
FTEs	**199.28**	**189.92**	**(9.36)**	**204.92**	**5.64**	**2.8%**

fund to reduce assessments, are determined annually as part of NERC's BP&B process, based on recommendation by the FAC and requiring both Board and FERC approval.

[20] Expanded Policy on Allocation of Certain Compliance and Enforcement Costs, July 29, 2008.

NERC's 2019 budget and funding requirements reflect the resources necessary to support achievement of the goals and objectives set forth in the *ERO Enterprise Operating Plan*. The 2019 budget is comprised of both operating and fixed asset (capital) costs. Operating costs generally include personnel, consulting, office space, software licensing, third-party data management, communications, and other customary services to support office operations. Fixed asset (capital) costs primarily reflect investments in equipment and software to support operations, including investments in the development of software applications and infrastructure to facilitate improved business processes and efficiency.

Key Budget Assumptions

Key assumptions used in the development of NERC's 2019 budget include the following:

- **A net increase to headcount by 6 (5.64 FTEs).** This reflects an increase of 11 positions (10.34 FTEs) in support of the long-term strategy for the E-ISAC, as outlined in the *Electricity Information Sharing and Analysis Center* section of Section A, and a decrease of 5 positions (4.70 FTEs) in the rest of NERC operations. A 6.0% reduction to FTEs (vacancy rate) is applied to account for attrition and hiring delays, which is the same as 2018.
- **Investment for the second year of the E-ISAC long-term strategy.** In addition to the headcount (FTE) increase for the E-ISAC discussed above, the strategy calls for investment in additional grid security exercise (GridEx) support, E-ISAC portal enhancements, and office facilities to support growth. Additional information can be found in *Exhibit E – E-ISAC Long-Term Strategy.*
- **Investments in technology and tools.** This includes a planned budget increase for the Compliance Monitoring and Enforcement Program (CMEP) tool, with investment in complementary solutions for entity registration and standards data, as described in *Exhibit F – CMEP Technology Project Business Case,* as well as an upgrade to a situational awareness tool, as outlined in *Exhibit G – Situation Awareness for FERC, NERC, and the Regional Entities (SAFNR)*.
- **Market-based compensation for personnel**. Executive and staff compensation and benefits are established based on guidelines established by the Board's Corporate Governance and Human Resources Committee (CGHRC) and the results of market compensation and benefit studies, most recently completed in 2017.
- **Anticipated market increases in medical and dental benefit plan costs**. Medical and dental premium cost estimates are based on market data provided by the company's benefits consultant. No other changes to retirement or other benefit plans have been assumed for 2019.
- **Meeting and travel expenses held flat.** The company has undertaken a number of significant efforts over the past several years to reduce travel and meeting expenses. For example, the company has worked closely with Regional Entities to share meeting space where possible, which has helped reduce meeting costs.

Fixed Asset (Capital) Budget and Capital Financing

NERC's 2019 capital budget is approximately $4.8M (excluding depreciation), which represents an increase of $904k from 2018. This increase is primarily due to additional ERO software project spending and leasehold improvements for the E-ISAC. The table below provides a summary of the major capital budget components.

NERC Capital Budget	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
ERO Application Development	$ 2,148,000	$ 3,268,000	$ 1,120,000	52.1%
Hardware (storage, servers)	805,000	565,000	(240,000)	-29.8%
Other Equipment	370,000	425,000	55,000	14.9%
Disaster Recovery	100,000	-	(100,000)	-100.0%
NERC Software Licenses	301,000	120,000	(181,000)	-60.1%
Leasehold Improvements	150,000	400,000	250,000	166.7%
Total	**$ 3,874,000**	**$ 4,778,000**	**$ 904,000**	**23.3%**

NERC has budgeted approximately $4.6M (both operating expenses and capital expenditures) in 2019 for services related to the planning, design, and implementation of software applications supporting ERO Enterprise tools for common NERC and Regional Entity operations. These related costs include approximately $3.3M in capital expenditures and $1.3M in other IT operating costs. Additional information regarding the ERO Enterprise IT strategy, the current status of the development of ERO Enterprise IT applications, and projects that will be under development in 2019 can be found in the *Information Technology* section of Section A. The 2019 capital budget also includes ongoing funding for IT security, data storage, servers, hardware, and software license costs.

CMEP Technology Project

Starting in 2017, NERC has been working closely with the Regional Entities to evaluate and implement strategic investments in tools that replace the current three CMEP applications used among NERC and the Regional Entities with a single, common CMEP application. Items under consideration include how Reliability Standards and entity registration data is stored and maintained, as well as how best to support the various parts of the compliance and enforcement process (e.g., analysis of risk, development of implementation plans and audit schedules, actual compliance monitoring, and enforcement processing).

Of the $3.3M in fixed asset (capital) expenditures for ERO Enterprise applications in 2019, approximately $1.8M relates to the new CMEP tool, with additional investments for complementary applications for entity registration ($600k) and standards data ($300k). The capital expenditure for the CMEP tool is expected to be approximately $5.0–6.0M in total, with work spanning through 2020. Funding for this work will be subject to review and approval as part of the BP&B process each year. For additional information on the CMEP Technology Project and entity registration and standards solutions, please see the *Information Technology* section of Section A, as well as *Exhibit F – CMEP Technology Project Business Case*.

SAFNR

The remaining 2019 capital expenditure of $600k for ERO Enterprise applications relates to enhancing the functionality of SAFNR to improve the ability to accurately understand current conditions on the BPS, and to incorporate functionality elements piloted during GridEx IV that will provide the E-ISAC with more timely and understandable common operating picture information. For additional information on SAFNR, please see the *Situation Awareness* section of Section A and *Exhibit G – Situation Awareness for FERC, NERC, and the Regional Entities (SAFNR)*.

The 2019 budget assumes that approximately $3.3M of the total $4.6M capital budget for ERO Enterprise applications will be financed through the capital financing program described and put in place as part of NERC's *2014 Business Plan and Budget*. Further information regarding capital financing can be found in *Exhibit C – Capital Financing*.

Working Capital and Operating Reserves

Under the company's *Working Capital and Operating Reserve Policy*, management is proposing an overall reserve budget of $8.8M for Working Capital (i.e., the amount of funds necessary to satisfy the company's projected cash flow needs during the budget year), the four categories of Operating Reserves, and the Assessment Stabilization Reserve. This represents an increase of $1.4M (18.2%) from the total reserve amounts included in NERC's 2018 budget. The reserve categories are broken down as follows:

- **Future Obligation Reserve** – Includes funding that has been received to satisfy future obligations under lease, credit, loan, or other agreements to which the company is a party. This reserve is comprised primarily of existing funds and is budgeted to be $2.0M for 2019.
- **System Operator Certification Reserve** – Includes surplus funding from operator certification and testing fees that are above incurred expenses and shall be used solely to support operator testing and certification needs. The 2019 System Operator Certification Reserve is budgeted at $644k and comprised primarily of existing funds.
- **CRISP Reserve** – Represents funds dedicated to support CRISP. These reserves are established pursuant to a CRISP budget agreed to and funded entirely by utilities participating in CRISP. These reserves have no impact on assessments and they are segregated from other reserves pursuant to the terms of the CRISP agreements. The CRISP reserves are projected to be $500k in the 2019 budget.
- **Operating Contingency Reserve** – Includes funds for contingencies that were not anticipated, assumed to be likely, or the timing of which was uncertain, at the time of preparation and approval of the company's BP&B. NERC's current policy on Operating Contingency Reserves requires a reserve target of 3.5–7.0%, except as otherwise approved by the Board after review and recommendation by the Board Finance and Audit Committee (FAC). This percentage is calculated against NERC's total budget for operating and capital expenditures, less those costs related to CRISP and System Operator Certification, each of which has a separate reserve category. For the 2019 budget, management is recommending an Operating Contingency Reserve of approximately $3.6M, or 4.5% of total budgeted operating and fixed asset (capital) costs.
- **Assessment Stabilization Reserve** – To date, this reserve has been funded entirely by previously received penalties and is projected to have a balance of $2.1M as of January 1, 2019. For purposes of the company's 2019 BP&B, management and the Board are considering the release of $564k of Assessment Stabilization Reserve funds to offset U.S. assessments. Assuming this occurs, the remaining balance of $1.5M in the Assessment Stabilization Reserve will be used to reduce U.S. assessments in one or more future periods, subject to review and approval by the Board and FERC in the applicable year's BP&B.

Department Budget and FTE Comparisons

The following table shows a 2019 versus 2018 total budget comparison by department. The amounts reflect all direct and indirect departmental costs, including fixed asset (capital) costs. Costs incurred for general and administrative and other overheads are considered indirect and are allocated to the statutory departments based on the ratio of that department's budgeted FTEs to total budgeted statutory FTEs.

2019 versus 2018 Total Budget by Department

Total Budget	2018 Budget	2019 Budget	Change 2019 Budget v 2018 Budget	% Change
Reliability Standards*	$ 6,821,893	$ 6,325,729	$ (496,165)	-7.3%
Compliance Monitoring and Enforcement Programs*	20,465,126	21,750,992	1,285,866	6.3%
Reliability Assessments and System Analysis	7,312,956	7,994,779	681,823	9.3%
Reliability Risk Management*	13,641,560	13,983,919	342,359	2.5%
Training, Education, and Personnel Certification	3,043,024	2,693,523	(349,501)	-11.5%
NERC Budget, excluding E-ISAC	**$ 51,284,559**	**$ 52,748,942**	**$ 1,464,384**	**2.9%**
E-ISAC (non-CRISP)	$ 13,130,686	$ 18,316,666	$ 5,185,980	39.5%
E-ISAC (CRISP)*	8,719,912	8,983,897	263,986	3.0%
Total E-ISAC Budget	**$ 21,850,597**	**$ 27,300,563**	**$ 5,449,966**	**24.9%**
Total Budget	**$ 73,135,156**	**$ 80,049,506**	**$ 6,914,350**	**9.5%**

**Includes key technology application costs, including the CMEP Technology Project and complementary solutions for entity registration and standards data, as well as SAFNR, for which funding is shared by Reliability Risk Management and E-ISAC.*

The primary areas of increase are in CMEP and E-ISAC. The increase in CMEP is primarily due to the capital costs associated with development of the CMEP and entity registration applications, as further discussed in the *Information Technology* section of Section A and *Exhibit F – CMEP Technology Project Business Case*. The E-ISAC increase reflects additional staff related to the long-term strategy discussed in the *Electricity Information Sharing and Analysis Center* section of Section A and the attachment to Exhibit E, *Expanding E-ISAC Operations to Include 24x7 Onsite Operations.* The increase for 2019 due to the implementation of this strategy is approximately $3.5M; most of the remaining increase is due to the allocation of general and administrative overhead costs based on the additional FTEs.

The decrease in the Reliability Standards and Training, Education, and Personnel Certification departments is largely the result of the elimination or reallocation of FTEs from these departments as part of the ongoing process to better align resources to support operating goals and risk priorities, which also results in lower indirect costs and allocation of fixed assets to these departments.

The following table presents a 2019 versus 2018 comparison of budgeted FTEs by department and reflects 2019 personnel additions, interdepartmental transfers of previously budgeted positions, and attrition assumptions. The number of FTEs represents the number of employees employed full time during the year, plus the number of employees employed part time (less than full schedule) or during a portion of the year, converted to a full-time basis. Headcount represents the total number of personnel employed during the year, regardless of the length of their employment or whether they are full-time or part-time employees. FTEs will be less than headcount, unless there are no part-time employees and no employees who are employed less than a full year. The company's 2019 personnel budget is based upon existing headcount and associated compensation and benefit costs, as well as assumptions on the number and cost of new hires and the assumed vacancy rate, all within an overall FTE budget. An average vacancy rate is applied to each position and its associated costs to arrive at an overall personnel cost budget. The vacancy rate represents an adjustment, which is applied in the calculation of budgeted personnel costs to account for attrition and for variations from the budget assumptions on the timing of new hires.

2019 versus 2018 FTEs by Department

FTEs*	2018 Budget	2019 Budget	Change 2019 Budget v 2018 Budget	% Change
Reliability Standards	15.51	13.63	(1.88)	-12.1%
Compliance Monitoring and Enforcement Programs	40.89	40.89	-	0.0%
Reliability Assessments and System Analysis	14.10	15.04	0.94	6.7%
Reliability Risk Management	26.32	25.38	(0.94)	-3.6%
Training, Education, and Personnel Certification	5.88	4.94	(0.94)	-16.0%
Administrative Programs	67.45	67.45	-	0.0%
NERC FTEs, excluding E-ISAC	**170.14**	**167.32**	**(2.82)**	**-1.7%**
E-ISAC (non-CRISP)	25.38	33.84	8.46	33.3%
E-ISAC (CRISP)	3.76	3.76	-	0.0%
Total E-ISAC FTEs	**29.14**	**37.60**	**8.46**	**29.0%**
Total FTEs	**199.28**	**204.92**	**5.64**	**2.8%**

**Reflects 2019 additions and transfers between departments, anticipated timing of 2019 hires, and assumes 6% attrition in all programs*

In 2019, there will be an increase of 11 positions in support of the long-term strategy for the E-ISAC, which includes 9 positions in the E-ISAC and 2 in the Administrative Programs area (see the *Electricity Information and Analysis Center* section of Section A for details). There will also be a decrease of 5 open positions in the remaining NERC departments. This results in an increase of 9 positions (8.46 FTEs) in the E-ISAC, a net decrease of 3 positions (2.82 FTEs) in other NERC departments (decrease of 5 positions plus the 2 support roles for E-ISAC), resulting in a total net increase of 6 positions (5.64 FTEs) for NERC in 2019. The table above reflects the elimination of 5 open positions and reallocations of staff. The proposed position eliminations and overall resource allocations will be undergoing further strategic evaluation during the budget development process.

Administrative Programs includes the Information Technology, Legal and Regulatory, Finance and Accounting, Human Resources, Facilities and Meeting Planning, Communications, External Affairs, and Government Relations staff. It also includes General and Administrative functions, which include the CEO, the Chief Reliability Officer (CRO), and their support staff. For FERC and external reporting purposes, these programs are allocated as indirect expenses to the operating areas on a per FTE basis.

The 2019 organizational chart can be found in Appendix 1**.** The difference between the number of positions reflected in the organizational chart and total budgeted FTEs is due to assumptions regarding vacancy rates and timing of new hires.

The following table includes a statement of activities comparing the 2018 budget, 2018 projection, and 2019 budget.

Statement of Activities and Fixed Assets Expenditures 2018 and 2019 Budgets

STATUTORY

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)	% Inc 2019 over 2018
Funding						
ERO Funding						
NERC Assessments	$ 62,936,968	$ 62,936,968	$ -	$ 69,449,054	$ 6,512,086	**10.3%**
Assessment Stabilization Reserve - Penalties	600,000	600,000	-	-	(600,000)	
Total NERC Funding	**$ 63,536,968**	**$ 63,536,968**	**$ -**	**$ 69,449,054**	**$ 5,912,086**	
Third-Party Funding (CRISP)	$ 7,324,253	$ 7,225,735	$ (98,518)	$ 7,456,449	$ 132,196	
Testing Fees	1,790,000	1,728,075	(61,926)	1,790,000	-	
Services & Software	50,000	50,000	-	40,000	(10,000)	
Workshops	185,000	185,000	-	195,000	10,000	
Interest	95,000	292,439	197,438	185,000	90,000	
Miscellaneous	-	-	-	-	-	
Total Funding (A)	**$ 72,981,221**	**$ 73,018,216**	**$ 36,995**	**$ 79,115,503**	**$ 6,134,282**	**8.4%**
Expenses						
Personnel Expenses						
Salaries	$ 31,791,098	$ 31,810,707	$ 19,609	$ 33,960,220	$ 2,169,123	
Payroll Taxes	1,949,557	1,905,115	(44,442)	2,062,799	113,242	
Benefits	3,988,886	4,206,507	217,621	4,691,914	703,027	
Retirement Costs	3,239,565	3,528,619	289,054	3,435,513	195,949	
Total Personnel Expenses	**$ 40,969,105**	**$ 41,450,947**	**$ 481,842**	**$ 44,150,446**	**$ 3,181,341**	**7.8%**
Meeting Expenses						
Meetings	$ 1,071,500	$ 1,071,500	$ -	$ 1,071,500	$ 0	
Travel	2,204,000	2,149,228	(54,772)	2,184,000	(20,000)	
Conference Calls	119,600	110,625	(8,975)	139,900	20,300	
Total Meeting Expenses	**$ 3,395,100**	**$ 3,331,353**	**$ (63,747)**	**$ 3,395,400**	**$ 300**	**0.0%**
Operating Expenses						
Consultants & Contracts	$ 13,724,185	$ 14,096,841	$ 372,656	$ 14,927,318	$ 1,203,133	
Office Rent	3,091,804	3,087,919	(3,885)	3,335,058	243,254	
Office Costs	5,365,084	5,290,720	(74,363)	6,550,137	1,185,053	
Professional Services	2,537,500	2,491,696	(45,804)	2,636,975	99,475	
Miscellaneous	39,500	39,500	-	62,000	22,500	
Depreciation	1,594,299	1,594,299	-	3,446,022	1,851,724	
Total Operating Expenses	**$ 26,352,371**	**$ 26,600,975**	**$ 248,604**	**$ 30,957,511**	**$ 4,605,139**	**17.5%**
Total Direct Expenses	**$ 70,716,577**	**$ 71,383,275**	**$ 666,699**	**$ 78,503,357**	**$ 7,786,781**	**11.0%**
Indirect Expenses	**$ 0**	**$ -**	**$ (0)**	**$ 0**	**$ (0)**	
Other Non-Operating Expenses	**$ 138,878**	**$ 138,878**	**$ -**	**$ 214,171**	**$ 75,293**	**54.2%**
Total Expenses (B)	**$ 70,855,455**	**$ 71,522,153**	**$ 666,699**	**$ 78,717,528**	**$ 7,862,074**	**11.1%**
Change in Assets	**$ 2,125,766**	**$ 1,496,063**	**$ (629,704)**	**$ 397,975**	**$ (1,727,792)**	
Fixed Assets						
Depreciation	$ (1,594,299)	$ (1,594,299)	$ -	$ (3,446,022)	$ (1,851,724)	
Computer & Software CapEx	2,549,000	2,549,000	-	3,488,000	939,000	
Furniture & Fixtures CapEx	-	-	-	-	-	
Equipment CapEx	1,175,000	1,175,000	-	890,000	(285,000)	
Leasehold Improvements	150,000	150,000	-	400,000	250,000	
Allocation of Fixed Assets	0	-	(0)	0	(0)	
Inc(Dec) in Fixed Assets (C)	**$ 2,279,701**	**$ 2,279,701**	**$ (0)**	**$ 1,331,978**	**$ (947,724)**	**-41.6%**
TOTAL BUDGET (=B+C)	**$ 73,135,156**	**$ 73,801,855**	**$ 666,699**	**$ 80,049,506**	**$ 6,914,350**	**9.5%**
TOTAL CHANGE IN WORKING CAPITAL (=A-B-C)*	**$ (153,935)**	**$ (783,639)**	**$ (629,704)**	**$ (934,003)**	**$ 1,071,656**	
FTEs	**199.28**	**189.92**	**(9.36)**	**204.92**	**5.64**	**2.8%**

* *Refer to Table B-1 for a complete analysis of the Working Capital and Operating Reserve balance.*

FERC Order 830 – Geomagnetic Disturbance

In FERC's Order No. 830 approving Reliability Standard TPL-007-1 (*Transmission System Planned Performance for Geomagnetic Disturbance Events*),[21] FERC directed NERC to file a research work plan describing how NERC will conduct research into the specific geomagnetic disturbance (GMD)-related topics identified in the order. Since that time, NERC developed a preliminary GMD research work plan containing a set of GMD research activities, which was filed with FERC on May 30, 2017 in accordance with the Order No. 830 directive. The research activities identified in the preliminary plan are expected to advance the understanding of GMD events and the risks these high-impact, low-frequency events pose to the reliability of the BPS. In October 2017, FERC issued an order accepting NERC's preliminary work plan.

NERC developed a research plan[22] with the Electric Power Research Institute (EPRI) and filed it with FERC on April 19, 2018. This $3.4M research project is being co-funded by NERC ($200k per year for three years) along with more than 20 owners and operators from the electric industry. Further, NERC continues to work with industry to collect information about geomagnetically induced current (GIC) and the potential impacts on power system reliability.

NERC has also worked with the technical committees to develop an ROP Section 1600 Data Request for the collection of GMD data, as directed by FERC in Order 830. The GMD Data Request will be presented to the NERC Board for approval in 2018. NERC has begun developing requirements for the necessary technology application to collect GMD data from reporting entities. These requirements will be used to determine future funding needs.

NERC continues to conduct outreach with representatives from governmental agencies in the U.S., Europe, and Canada, academia, vendors, and industry to identify the GMD-related work that is currently in progress and determine where opportunities exist for research synergies.

E-ISAC Long-Term Strategy

Over the past several years the E-ISAC has focused on improving its technical and analytical capabilities with a goal of becoming the electricity industry's leading, trusted source for analysis and sharing of security information. Significant support from the Electricity Subsector Coordinating Council (ESCC), the ESCC Members Executive Committee (MEC)[23], the DOE, and other stakeholders have helped the E-ISAC provide the industry with unique insights, leadership, and coordination on security matters.

At the request of the NERC Board and under the guidance of the ESCC and MEC, executive leadership of the E-ISAC developed a long-term strategic plan, which is included as *Exhibit E – E-ISAC Long-Term Strategy*. The long-term strategic plan is to transform the E-ISAC into a world-class intelligence collecting and analytical capability for the electricity industry. The *E-ISAC Long-Term Strategy* was approved by the MEC on April 24, 2017 and accepted by the Board on May 11, 2017.

To carry forth this vision, the E-ISAC is planning a continuous and deliberate growth strategy over the next four years that increases both staff and technical resources. Based on industry and stakeholder feedback, the 2019 BP&B includes the second year's recommended additions related to this strategy, primarily related to analytical capabilities, as further described in the *Electricity Information Sharing and Analysis Center* section of Section A and the attachment to Exhibit E, *Expanding E-ISAC Operations to Include 24x7 Onsite Operations*.

---

[21] FERC Order 830 - Reliability Standard for Transmission System Planned Performance for Geomagnetic Disturbance Events

[22] Revised Geomagnetic Disturbance Research Work Plan of the North American Electric Reliability Corporation

[23] The ESCC formed the MEC in March 2016 to provide industry leadership and expertise to guide and support the E-ISAC, including but not limited to the development of strategic plans and budgets.

Projections for 2020–2021

Management is currently developing preliminary operating and fixed asset (capital) projections for 2020 and 2021. Assumptions considered in preparing these projections will include impacts of the long-term E-ISAC strategy discussed in *Exhibit E – E-ISAC Long-Term Strategy*, personnel and benefit cost increases, consultant and contract expenses, facility and software maintenance costs, as well as work related to the CMEP Technology Project, which is expected to continue through 2020 (see *Exhibit F – CMEP Technology Project Business Case* for more details).

Further details on projections will be provided in the second draft of the 2019 BP&B, with the general expectation that 2020 and 2021 will have less upward pressure than 2019. Additionally, during the 2020 and 2021 budget process, NERC will continue the goal of aligning assessments and budget increases through Assessment Stabilization Reserve releases so that year-to-year variations in receipt of penalties do not cause large year-to-year variations in future U.S. assessments.

Reliability Standards

Reliability Standards Program (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	15.51	13.63	(1.88)
Direct Expenses	$ 3,332,944	$ 3,201,759	$ (131,185)
Indirect Expenses	3,470,011	3,203,034	(266,977)
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	18,939	(79,064)	(98,003)
TOTAL BUDGET	$ 6,821,893	$ 6,325,729	$ (496,165)

Background and Scope

The Reliability Standards program carries out the ERO's statutory responsibility to develop, adopt, obtain approval of, and modify (as and when appropriate) mandatory NERC Reliability Standards (both continent-wide standards and regional reliability standards) to assure the BES is planned, operated, maintained, and secured to minimize risks of cascading failures, avoid damage to major equipment, or limit interruptions of the BPS. The major activities undertaken by the Standards department include:

- **Delivering high-quality, continent-wide reliability standards**: NERC standard developers and other standards staff provide project management and leadership to develop solutions necessary to address reliability risks identified through the Reliability Risk Management Process (RRMP). These may include the development of, or modifications to, Reliability Standards through standard development outreach activities, facilitation of drafting team activities, drafting support, assisting drafting teams in maintaining adherence to the development process as outlined in the *Standard Processes Manual*, and ensuring that the quality of documents produced is appropriate for approval by industry and the Board. Compliance Assurance continues to work closely with the standard development program to provide compliance information, statistics, technical input, and perspectives to drafting teams to clarify compliance risks.
- **Facilitating continent-wide industry engagement**: NERC manages the work of over 200 industry contributors who serve on the Standards Committee, subgroups, and other project teams for the development of Reliability Standards through the standards development program.
- **Conducting balloting, disseminating information, and supporting regulatory filings**: Through NERC's commenting and ANSI-accredited balloting process, industry consensus is built by engaging thousands of industry volunteers within hundreds of registered entities throughout North America who review, comment on, and approve the standards created by the standard drafting teams. The department also supports the filing of standards with applicable regulatory authorities and provides support with regulatory proceedings.

The Reliability Standards program provides a mechanism for the Regional Entities to process regional standards when unique regional reliability gaps are detected, or incorporate regional variances into continent-wide standards. The NERC Standards department staff supports regional standards development processes by providing technical advice, final quality review of regional standards, presentation to the Board, and preparation of regional standards materials for submission for standard adoption to the applicable regulatory authorities in the U.S. and Canada.

Stakeholder Engagement and Cost Effectiveness Project

As part of the standard development process, industry technical experts scope, draft, and review the new or revised Reliability Standards for approval by the industry ballot body, adoption by the Board, and filing with regulatory authorities in the U.S. and Canada. Additionally, federal, state and provincial regulatory authorities, the Board, Regional Entities, and many industry stakeholders have expressed interest in the identification of costs incurred from implementing Reliability Standards compared to risks they address. The objective is to ensure that these elements are considered during the standards development and revision process. A process has been established that ensures that industry feedback on costs is taken into account throughout the standard development process.

Key Efforts Underway

NERC ensures that the Reliability Standards Development Plan (RSDP) is effectively executed and that Reliability Standards are focused on and mitigate significant risks to BES reliability. Department resources are focused on supporting the *ERO Enterprise Operating Plan*, including but not limited to support of the RRMP and resolving FERC directives. Standards department key activities include:

- **Focus on the selection of projects undertaken.** Resources are expended on issues determined to be a reliability risk through the RRMP (also see the Reliability Assessment and System Analysis section and the Performance Analysis section below for additional detail). The department applies broad project management skills to implement a variety of solutions to a reliability concern. An effective solution to an identified reliability risk may be a Reliability Standard, or it may be a guideline, information request, training, NERC Alert, technical conference, research, or a combination of these or other tools.
- **Address FERC directives and respond to FERC orders** through standard development projects, as necessary. Each project determines whether: (1) the directive will be complied with as issued, (2) there is an equally effective and efficient way to address the concern that fostered the directive, or (3) there is technical justification (including that the directive has been overcome by events, processes, or advances in technology) that resolution of the directive is no longer needed.
- **Perform a comprehensive review of standards.** In 2018, NERC and industry will complete a comprehensive review of the Reliability Standards to measure their effectiveness and ability to mitigate the risks to the reliability and security of the BPS, compared to the industry burden for their implementation. An outcome of this review will inform the need to retire or enhance requirements based on operational experience. This will include an analysis of reliability risk, particularly emerging risks, and cost effectiveness. In 2019, projects will be initiated to address the results of this review to retire or modify Reliability Standards.
- **Facilitate smooth transition to new standards**. This includes working with the Compliance Assurance, Enforcement, Registration, Reliability Assurance, Reliability Assessment and System Analysis, and Performance Analysis groups to develop guidelines, webinars, and other activities to support auditor and industry training for the new standards.

The 2019–2021 RSDP will be developed in 2018 in conjunction with the Standards Committee, RISC, and RRMP. It will outline the work plan for the continued evaluation of Reliability Standards, the Standards department's support of Reliability Risk Management, and resolution of FERC directives. Additionally, standards grading metrics will be used to measure the overall quality of each enforceable Reliability Standard as a basis for measuring needed improvements.

2019 Goals and Deliverables

In 2018, the body of Reliability Standards will be reviewed for potential improvements while considering quality and content criteria, as well as results-based standards principles. In 2019, industry and NERC will determine whether there is a need to make further improvements to the standards through periodic reviews that include: (1) a measured review of the content of standards, considering whether the requirements could more effectively mitigate risks to the BPS, (2) whether the standards are results-based and drafted with high quality, (3) whether the standards are concise or if the number of requirements could be reduced, and (4) whether compliance expectations are clear. Also in 2019, Standards staff will continue to support the operating plan through the key activities discussed above by addressing potential improvements, any new directives issued by FERC, as well any reliability risks identified through RRMP or by the RISC for which a Reliability Standard is part of the solution.

Resource Requirements

Personnel

The 1.88 reduction in FTEs results from the elimination of an open position (0.94 FTEs) and reallocation of one position (0.94 FTEs) to realign staff with current needs.

Consultants and Contracts

No consultant or contract expenses were budgeted in 2018. Budgeted consultant and contract expenses are $50k for 2019 for standards development support. A detailed breakdown of 2018 and 2019 budgeted expenses is shown in *Exhibit B – Consultant and Contractor Costs*.

Other Costs

The $300k increase in computer and software capital expenditures is for a standards database solution in support of the CMEP Technology Project.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
RELIABILITY STANDARDS

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 6,689,437	$ 6,689,437	$ -	$ 6,248,095	$ (441,342)
Assessment Stabilization Reserve - Penalties	71,739	71,739	-	-	(71,739)
Total NERC Funding	**$ 6,761,176**	**$ 6,761,176**	**$ -**	**$ 6,248,095**	**$ (513,082)**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	50,000	50,000	-	60,000	10,000
Interest	10,717	8,038	(2,679)	17,634	6,917
Miscellaneous	-	-	-	-	-
Total Funding	**$ 6,821,893**	**$ 6,819,214**	**$ (2,679)**	**$ 6,325,729**	**$ (496,165)**
Expenses					
Personnel Expenses					
Salaries	$ 2,207,431	$ 1,815,391	$ (392,039)	$ 1,901,684	$ (305,746)
Payroll Taxes	145,638	118,131	(27,507)	125,885	(19,753)
Benefits	299,194	257,208	(41,986)	274,307	(24,887)
Retirement Costs	246,107	231,187	(14,920)	210,408	(35,699)
Total Personnel Expenses	**$ 2,898,370**	**$ 2,421,917**	**$ (476,453)**	**$ 2,512,285**	**$ (386,086)**
Meeting Expenses					
Meetings	$ 105,000	$ 105,000	$ -	$ 105,000	$ -
Travel	240,000	238,050	(1,950)	220,000	(20,000)
Conference Calls	-	1,492	1,492	18,000	18,000
Total Meeting Expenses	**$ 345,000**	**$ 344,542**	**$ (458)**	**$ 343,000**	**$ (2,000)**
Operating Expenses					
Consultants & Contracts	$ -	$ 100,000	$ 100,000	$ 50,000	$ 50,000
Office Rent	-	-	-	-	-
Office Costs	49,796	27,328	(22,468)	38,200	(11,596)
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	39,278	39,278	-	257,774	218,496
Total Operating Expenses	**$ 89,574**	**$ 167,106**	**$ 77,532**	**$ 346,474**	**$ 256,900**
Total Direct Expenses	**$ 3,332,944**	**$ 2,933,565**	**$ (399,378)**	**$ 3,201,759**	**$ (131,185)**
Indirect Expenses	**$ 3,470,011**	**$ 3,268,555**	**$ (201,456)**	**$ 3,203,034**	**$ (266,977)**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 6,802,955**	**$ 6,202,121**	**$ (600,834)**	**$ 6,404,793**	**$ (398,162)**
Change in Assets	**$ 18,939**	**$ 617,093**	**$ 598,155**	**$ (79,064)**	**$ (98,003)**
Fixed Assets					
Depreciation	$ (39,278)	$ (39,278)	$ -	$ (257,774)	$ (218,496)
Computer & Software CapEx	-	-	-	300,000	300,000
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	58,217	53,498	(4,718)	(121,290)	(179,507)
Inc(Dec) in Fixed Assets (B)	**$ 18,939**	**$ 14,220**	**$ (4,718)**	**$ (79,064)**	**$ (98,003)**
TOTAL BUDGET (=A+B)	**$ 6,821,893**	**$ 6,216,341**	**$ (605,552)**	**$ 6,325,729**	**$ (496,165)**
FTEs	**15.51**	**13.38**	**(2.13)**	**13.63**	**(1.88)**

Compliance Assurance, Compliance Analysis, Organization Registration and Certification, and Compliance Enforcement

The Compliance Assurance, Compliance Analysis, Organization Registration and Certification, and Compliance Enforcement program areas promote a culture of reliability excellence through risk-informed compliance monitoring, mitigation, enforcement, and registration.

Compliance Assurance

Compliance Assurance (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	19.27	19.27	-
Direct Expenses	$ 4,520,550	$ 4,957,266	$ 436,717
Indirect Expenses	4,311,226	4,528,428	217,202
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	72,330	712,521	640,191
TOTAL BUDGET	$ 8,904,105	$ 10,198,215	$ 1,294,110

Background and Scope

NERC's Compliance Assurance group works collaboratively with the Regional Entities to ensure effective implementation of risk-based compliance monitoring under the CMEP across the entire ERO Enterprise. This program ensures that Regional Entities monitor registered entities for compliance according to their own specific facts and circumstances, including the entity's inherent risks, evaluation of controls in place to mitigate the inherent risks, and other factors, such as risk elements and entity performance. Additionally, the risk-based compliance monitoring approach allows for the appropriate allocation of resources to the issues that pose a higher level of risk to the reliability of the BPS.

The CMEP provides for Regional Entities to develop customized compliance oversight plans (COPs) for each registered entity that identifies: (1) the standards or requirements to be monitored; (2) the monitoring processes (tools) for use by the Regional Entities, including compliance audits, self-certification, and spot checking; and (3) the interval of monitoring. NERC and the Regional Entities ensure that inherent risk assessments (IRAs) for registered entities begin with a consistent framework and that Regional Entities' implementation of the CMEP coalesce around effective and efficient practices, ensuring comprehensive data management procedures that address data reporting requirements, integrity, retention, security, and confidentiality.

The Compliance Assurance group's responsibilities include, but are not limited to, the following major activities and functions:

- Oversight of the Regional Entities' implementation of the risk-based compliance monitoring program and NERC ROP in North America;
- Development and execution of the annual CMEP Implementation Plan (IP);
- Oversight of the use of necessary compliance-related processes, procedures, IT platforms, tools, and templates;
- Development and delivery of education and training for ERO Enterprise staff;

- Training and outreach activities for the Critical Infrastructure Protection (CIP) Reliability Standards and subsequent enhancements to support industry compliance and security;
- Coordination with the NERC Standards department to assist in the smooth transition for standards from development to enforceability and feedback on risks seen in the field that are not addressed by a standard, as well as information on where a standard is too broad; and
- Support for Regional Entity and industry committees, working groups, and task forces, such as the ERO Compliance Monitoring Group, NERC Compliance and Certification Committee (CCC) and NERC Critical Infrastructure Protection Committee (CIPC).

Stakeholder Engagement and Benefit

NERC continues to promote the Regional Entities' development of customized COPs for registered entities. As the risk-based compliance monitoring approach was implemented in 2015 and 2016, Regional Entities worked closely with stakeholders to develop IRAs and appropriately scope compliance monitoring activities. As this process continues to mature, Regional Entities will continue to customize compliance monitoring tools and frequency of monitoring for each registered entity, based on its IRA as well as additional considerations such as risk elements, entity performance, internal controls, and mitigating activities to inform the development of their COPs.

Compliance Assurance continues to work closely with the standard development program to provide compliance information, statistics, technical input, and perspectives to drafting teams to provide an increased reliability benefit and clarify compliance risks. This collaboration with industry and the Standards department occurs early in the standard development process by providing draft compliance monitoring insights, including information on how compliance with draft standards will be determined, as well as input to the drafting teams on the auditability and enforceability of the draft standards. This collaboration ensures that ERO Enterprise tools used in the auditing process, such as the reliability standards auditing worksheet (RSAW), do not expand or modify standards requirements.

NERC also continues to provide industry-focused outreach events and webinars on the ERO Enterprise's approaches to risk-based CMEP activities. ERO Enterprise staff will continue its webinar series providing views on standards and requirements associated with the 2019 risk elements identified for consideration for compliance monitoring.

Key Efforts Underway

NERC Oversight of Risk-Based Compliance Monitoring

Consistent with the goals and objectives set forth in the operating plan, NERC continues to implement risk-based compliance monitoring as part of its stated objectives of ensuring BPS reliability, improving consistency, effectiveness, and efficiency of ERO Enterprise compliance operations, focusing on identified risks, and reducing unnecessary burdens on registered entities. Ensuring the successful implementation of NERC's risk-based CMEP remains the priority of Compliance Assurance's oversight plan for the Regional Entities. As part of that oversight, and in addition to offering regular feedback to the Regional Entities, NERC continues to identify areas for improvement or promoting consistency through training, guidance, or adjustments during the following year. NERC also produces an ERO Enterprise CMEP annual report, which includes an assessment of the risk-based CMEP implementation.

NERC performs oversight of the Regional Entities' compliance monitoring programs primarily through the review of processes, supporting evidence, observations, and other information provided by the Regional Entities over the course of focused program area engagements that are scheduled throughout the year. NERC communicates the recommendations and findings to the Regional Entities to help the ERO

Enterprise develop responsive strategies and solutions to potential issues and ensure uniform and consistent implementation of the CMEP. Such recommendations and findings also help identify priority areas for training of ERO Enterprise staff during the year.

CIP Compliance
NERC and the Regional Entities continue to manage the smooth implementation of compliance activities for CIP Version 5 Reliability and Physical Security Standards, along with their subsequent enhancements by providing training, webinars, and other forms of outreach. The ERO Enterprise continues to provide educational programs to support industry compliance and the integration of risk assessment and internal controls.

CMEP Technology Project
Beginning in 2017 through 2020, NERC, in collaboration with the Regional Entities, will develop and implement a common CMEP tool, including the various processes and activities (e.g., analysis of risk, development of implementation plans and audit schedules, actual compliance monitoring, and enforcement processing). For more information on the CMEP Technology Project, see the *Information Technology* section of Section A, as well as *Exhibit F – CMEP Technology Project Business Case*.

Regional Entity Training
NERC Compliance Assurance provides training to Regional Entity staff on the most important elements of risk-based compliance monitoring, including enhancements to registered entity IRAs, internal controls reviews, COP development, as well as Reliability Standards monitoring. NERC develops this training based on observations from its oversight activities of the Regional Entities, as well as the process reviews described above.

Emerging Technology Roundtables
Compliance Assurance periodically hosts an Emerging Technology Roundtable with industry and vendors that includes in-depth discussions around the integration of emerging technologies associated with BPS operations to address and mitigate cyber and physical security risks of the BPS.

Compliance Enforcement Authority for Southwest Power Pool Regional Transmission Organization
As a result of the Southwest Power Pool Regional Entity (SPP RE) dissolution process, in early 2018 the Board approved, and FERC subsequently approved,[24] that NERC assume the Compliance Enforcement Authority (CEA) activities for the registered entity SPP Regional Transmission Organization (RTO) for two years. This is the role that is generally delegated by NERC to a Regional Entity. Essentially the CEA is responsible for planning and conducting all CMEP activities as described in the ROP and other guiding documents. NERC will leverage existing internal and Regional Entity resources and expertise to undertake the CEA activities with respect to the SPP RTO.

2019 Goals and Deliverables

The Compliance Assurance group has several goals and deliverables that support the *ERO Enterprise Operating Plan.* Resources will be focused on improvements implemented as a result of the risk-based compliance monitoring activities in 2017 and 2018. Specific 2019 objectives for this group are:

- Continue to mature the risk-based compliance monitoring program, providing ongoing oversight of the risk-based CMEP, including IRAs, consideration of internal controls, coordinated oversight of Multi-Region Registered Entities (MRREs), and ensuring that COPs are addressing the relevant risks.

[24] *North American Electric Reliability Corporation, Midwest Reliability Organization, and SERC Reliability Corporation, Order Granting Approvals in Connection with the Dissolution of the Southwest Power Pool regional Entity*, 163 FERC ¶ 61,094 (2018).

- Work closely with NERC's Enforcement and IT departments, as well as staff in the Regional Entities, to develop application business requirements and test business functionality for the ERO Enterprise CMEP tool.
- Support the continued successful implementation of the CIP Version 5 Reliability Standards and subsequent enhancements as they become effective.
- Monitor and support effective implementation of the physical security Reliability Standard.
- Enhance and implement training to support monitoring of Reliability Standards, integrating principles from the Compliance Monitoring Competency Guide.
- Continue feedback to Standards through integration and coordination between the standards and compliance functions for clear stakeholder implementation and feedback on risks seen in the field that are not addressed by a standard, as well as information on where a standard is too broad. This effort will be supported through a common set of RSAWs, guidance, and outreach.
- Support international CMEP activities, including reliability and security subject matter expertise and outreach.
- Provide support and leadership to the CIPC and CCC as well as their subcommittees, working groups, and task forces. Support the CIPC and CCC leadership and development and implementation of annual work plans.
- Develop and implement the NERC CEA program for SPP RTO.

These 2019 activities are necessary to further implement risk-based compliance monitoring, including the CIP standards, and integrate the standards and compliance functions. A number of activities that support the implementation of the strategic risk-based reforms are intended to reduce regulatory burden by focusing compliance monitoring according to each registered entity's potential impact on the BPS.

Resource Requirements

Personnel

The increase in Compliance Assurance personnel in prior years through the reallocation of resources from other departments to Compliance Assurance was the result of NERC's plan to strengthen the implementation and oversight of the risk-based CMEP, increase risk analysis capabilities and technical expertise, and support feedback loops that improve program oversight and the development and implementation of Reliability Standards. Due to the maturation of these areas, two positions (1.88 FTEs) are being eliminated from the Compliance Assurance department. However, there is a net change of zero FTEs from 2018 to 2019 due to the reallocation of one position (0.94 FTEs) from another department to Compliance Assurance and the addition of an unbudgeted position (0.94 FTEs) to the Compliance Assurance department in 2018.

Consultants and Contracts

Funds budgeted for consultant and contract expenses to assist in successful implementation of risk-based compliance monitoring remains unchanged at $50k. A detailed breakdown of the 2018 and 2019 budgeted expenses is shown in *Exhibit B – Consultant and Contractor Costs*.

Other Costs

The $884k increase in computer and software capital expenditures is attributed to the CMEP Technology Project, for which the total capital expenditure of approximately $1.8M is split evenly between Compliance Assurance and Compliance Enforcement. The $273k increase in office costs is primarily for license and hosting fees for the new CMEP tool.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
COMPLIANCE ASSURANCE

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 8,801,659	$ 8,801,659	$ -	$ 10,173,284	$ 1,371,625
Assessment Stabilization Reserve - Penalties	89,130	89,130	-	-	(89,130)
Total NERC Funding	**$ 8,890,790**	**$ 8,890,790**	**$ -**	**$ 10,173,284**	**$ 1,282,494**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	13,316	9,987	(3,329)	24,931	11,616
Miscellaneous	-	-	-	-	-
Total Funding	**$ 8,904,105**	**$ 8,900,776**	**$ (3,329)**	**$ 10,198,215**	**$ 1,294,110**
Expenses					
Personnel Expenses					
Salaries	$ 2,936,161	$ 2,974,983	$ 38,822	$ 2,979,087	$ 42,927
Payroll Taxes	192,067	207,159	15,093	195,291	3,224
Benefits	398,424	477,882	79,458	504,583	106,159
Retirement Costs	324,835	356,270	31,436	328,205	3,371
Total Personnel Expenses	**$ 3,851,487**	**$ 4,016,295**	**$ 164,808**	**$ 4,007,166**	**$ 155,680**
Meeting Expenses					
Meetings	$ 200,000	$ 200,000	$ -	$ 200,000	$ -
Travel	375,000	335,856	(39,144)	375,000	-
Conference Calls	-	6,773	6,773	8,000	8,000
Total Meeting Expenses	**$ 575,000**	**$ 542,628**	**$ (32,372)**	**$ 583,000**	**$ 8,000**
Operating Expenses					
Consultants & Contracts	$ 50,000	$ 50,000	$ -	$ 50,000	$ -
Office Rent	-	-	-	-	-
Office Costs	43,563	37,687	(5,876)	316,600	273,037
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	-	-	-	-	-
Total Operating Expenses	**$ 94,063**	**$ 88,187**	**$ (5,876)**	**$ 367,100**	**$ 273,037**
Total Direct Expenses	**$ 4,520,550**	**$ 4,647,111**	**$ 126,561**	**$ 4,957,266**	**$ 436,717**
Indirect Expenses	**$ 4,311,226**	**$ 4,839,319**	**$ 528,093**	**$ 4,528,428**	**$ 217,202**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 8,831,775**	**$ 9,486,429**	**$ 654,654**	**$ 9,485,694**	**$ 653,919**
Change in Assets	**$ 72,330**	**$ (585,653)**	**$ (657,983)**	**$ 712,521**	**$ 640,191**
Fixed Assets					
Depreciation	$ -	$ -	$ -	$ -	$ -
Computer & Software CapEx	-	-	-	884,000	884,000
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	72,330	79,208	6,878	(171,479)	(243,809)
Inc(Dec) in Fixed Assets (B)	**$ 72,330**	**$ 79,208**	**$ 6,878**	**$ 712,521**	**$ 640,191**
TOTAL BUDGET (=A+B)	**$ 8,904,105**	**$ 9,565,637**	**$ 661,532**	**$ 10,198,215**	**$ 1,294,110**
FTEs	**19.27**	**19.81**	**0.54**	**19.27**	**-**

Compliance Analysis, Organization Registration and Certification

Compliance Analysis, Organization Registration and Certification (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	9.40	9.40	-
Direct Expenses	$ 2,148,762	$ 2,391,491	$ 242,729
Indirect Expenses	2,103,037	2,208,989	105,952
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	635,283	404,675	(230,608)
TOTAL BUDGET	$ 4,887,082	$ 5,005,155	$ 118,073

Background and Scope

The Compliance Analysis, Organization Registration, and Organization Certification functions are fulfilled by two groups at NERC: Registration and Reliability Assurance (includes Compliance Analysis and Organization Certification). The groups are responsible for a range of requirements and activities embodied in Section 500 (Organization Registration and Certification) and Appendices 5A and 5B of the NERC ROP. The groups provide technical resource support to the standards development, compliance monitoring, and enforcement functions. The following specific activities are conducted:

- **Registration** – Identify and register BES users, owners, and operators that are responsible for compliance with Reliability Standards. Organizations that are registered are included on the NERC Compliance Registry (NCR) and responsible for knowing the content of and complying with all applicable Reliability Standards. Maintain the current registry for the entire ERO as entities take on and drop functional responsibilities.
- **Certification** – Evaluate and certify the competency of reliability entities, i.e., RCs, BAs, and TOPs. Entities performing these functions must be evaluated for having the necessary personnel, knowledge, facilities, programs, and other qualifications to carry out these important responsibilities. For example, they must demonstrate the ability to meet the requirements and sub-requirements of all of the Reliability Standards applicable to the reliability function(s). This also includes confirming through the certification review process that a reliability entity continues to have the capabilities mentioned above following planned and unplanned material changes to that entity's operation.
- **Reliability assurance** – Conduct activities to reasonably assure the ERO that certain actions have been taken as reported in response to NERC Alerts or guidance to industry.
- **Oversight** – Provide oversight of Regional Entity implementation of regional registration, compliance, certification, investigation, complaint programs, and processes.
- **Investigations** – Conduct non-public, confidential investigations to identify possible violations of NERC Reliability Standards in response to complaints, BES disturbances, or other similar triggers. Registration and Reliability Assurance staff participate on all Regional Entity-led investigations and as observers as requested on FERC-led reliability investigations and inquiries.
- **Compliance evaluations** – Work closely with Regional Entity staff to confirm that qualified events and disturbances are evaluated against the relevant approved Reliability Standards and ensure formal compliance monitoring occurs if indicated. These analyses are shared with FERC staff.
- **Complaints** – Address formal complaints that allege the violation of Reliability Standards, through a confidential process.

Key Efforts Underway

Registration continues to implement areas for improvements identified in 2016. These areas included:

- Conducting NERC-led Review Panels on registration requests and identifying process improvements;
- NERC ROP changes;
- Reviewing the Coordinated Functional Registration (CFR) process and model efficiencies;
- Supporting the entity registration xRM database (centralized entity registration system) initiative;
- Conducting a thorough review of the NERC website for any registration-related modifications;
- Continuing Regional Entity oversight activities.

Additionally, on July 27, 2017, NERC issued a letter to entities registered in the SPP RE footprint that NERC and SPP had mutually agreed to terminate the delegation agreement between NERC and SPP RE. NERC Registration is leading this effort to transition these entities to other Regional Entities, which requires an extensive amount of time and resources. Work will continue throughout the majority of 2018 and into 2019.

NERC Reliability Assurance, in conjunction with Regional Entities, performed a review of the Certification program in 2016 regarding its effectiveness in determining an entity's ability to become certified and then operational, and to begin incorporating changes to the program, if applicable, based on the outcomes of the review. The team concluded that the certification process is necessary and is effective in determining an entity's ability to become certified and operational. The team recommended two improvements to the existing certification process which are continuing to be addressed:

- Clearly establish the focus of certification on evaluation of an entity's capability to perform the reliability function of TOP, BA, and/or RC through the use of standardized templates to be used by each Regional Entity's certification team.
- Conduct an evaluation of the certification review process to determine effectiveness of the current triggers of the certification review and execution of the actual process, and implement any needed ROP changes.
- Continue Regional Entity oversight activities.

2019 Goals and Deliverables

The Registration and Reliability Assurance groups have several goals and deliverables that support the *ERO Enterprise Operating Plan.* Resources will be focused on building upon the improvements identified in 2016 as well as the SPP RE transition. Specific 2019 objectives for these groups are:

- Continue to conduct NERC-led Review Panels on registration requests.
- Continue to implement Registration program improvements and conduct any additional actions identified by the project.
- Begin the entity registration xRM database initiative (centralized entity registration system).
- Continue to manage the SPP RE transition.
- Monitor and support changing footprints, functional relationships, and model changes in the Western Interconnection, especially with regard to the RC role.
- Ensure proper oversight of the Regional Entities for the Certification program.

- Respond to industry changes requiring certification review, with particular emphasis on control center relocations, Energy Management System (EMS) replacements, and RC, BA, and TOP footprint changes.
- Evaluate BES disturbances and events for potential gaps in compliance monitoring or Reliability Standards.
- Support the ongoing joint FERC, NERC, and Regional Entity restoration and recovery initiatives in conjunction with industry.

Resource Requirements

Personnel
No change in FTEs for 2019 from the 2018 budget.

Consultants and Contracts
No consultant or contract expenses are budgeted in 2019, which is consistent with the 2018 budget.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
COMPLIANCE ANALYSIS, ORGANIZATION REGISTRATION and CERTIFICATION

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 4,837,109	$ 4,837,109	$ -	$ 4,992,994	$ 155,885
Assessment Stabilization Reserve - Penalties	43,478	43,478	-	-	(43,478)
Total NERC Funding	**$ 4,880,587**	**$ 4,880,587**	**$ -**	**$ 4,992,994**	**$ 112,407**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	6,495	4,872	(1,624)	12,162	5,666
Miscellaneous	-	-	-	-	-
Total Funding	**$ 4,887,082**	**$ 4,885,458**	**$ (1,624)**	**$ 5,005,155**	**$ 118,073**
Expenses					
Personnel Expenses					
Salaries	$ 1,514,712	$ 1,570,903	$ 56,190	$ 1,596,696	$ 81,983
Payroll Taxes	95,616	96,821	1,205	98,909	3,293
Benefits	194,709	217,793	23,084	230,401	35,692
Retirement Costs	168,791	194,928	26,137	178,558	9,767
Total Personnel Expenses	**$ 1,973,828**	**$ 2,080,445**	**$ 106,617**	**$ 2,104,565**	**$ 130,736**
Meeting Expenses					
Meetings	$ 2,250	$ 2,250	$ -	$ 2,250	$ -
Travel	150,500	148,907	(1,593)	150,500	-
Conference Calls	-	2,982	2,982	5,400	5,400
Total Meeting Expenses	**$ 152,750**	**$ 154,139**	**$ 1,389**	**$ 158,150**	**$ 5,400**
Operating Expenses					
Consultants & Contracts	$ -	$ 49,950	$ 49,950	$ -	$ -
Office Rent	-	-	-	-	-
Office Costs	21,684	21,724	40	16,600	(5,084)
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	-	-	-	111,677	111,677
Total Operating Expenses	**$ 22,184**	**$ 72,174**	**$ 49,990**	**$ 128,777**	**$ 106,592**
Total Direct Expenses	**$ 2,148,762**	**$ 2,306,759**	**$ 157,996**	**$ 2,391,491**	**$ 242,729**
Indirect Expenses	**$ 2,103,037**	**$ 2,328,052**	**$ 225,015**	**$ 2,208,989**	**$ 105,952**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 4,251,799**	**$ 4,634,810**	**$ 383,011**	**$ 4,600,480**	**$ 348,681**
Change in Assets	**$ 635,283**	**$ 250,648**	**$ (384,635)**	**$ 404,675**	**$ (230,608)**
Fixed Assets					
Depreciation	$ -	$ -	$ -	$ (111,677)	$ (111,677)
Computer & Software CapEx	600,000	600,000	-	600,000	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	35,283	38,105	2,822	(83,648)	(118,931)
Inc(Dec) in Fixed Assets (B)	**$ 635,283**	**$ 638,105**	**$ 2,822**	**$ 404,675**	**$ (230,608)**
TOTAL BUDGET (=A+B)	**$ 4,887,082**	**$ 5,272,915**	**$ 385,833**	**$ 5,005,155**	**$ 118,073**
FTEs	**9.40**	**9.53**	**0.13**	**9.40**	**-**

Compliance Enforcement

Compliance Enforcement (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	12.22	12.22	-
Direct Expenses	$ 2,451,137	$ 3,005,692	$ 554,555
Indirect Expenses	2,733,948	2,871,686	137,738
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	1,488,854	670,243	(818,610)
TOTAL BUDGET	$ 6,673,939	$ 6,547,621	$ (126,317)

Background and Scope

The NERC Enforcement group is responsible for overseeing enforcement processes, the application of penalties or sanctions, and activities to mitigate and prevent recurrence of noncompliance with Reliability Standards. The group works collaboratively with the Regional Entities to ensure consistent and effective implementation of the risk-based CMEP. Importantly, the department also focuses on ensuring that the ERO Enterprise dedicates resources to the matters that pose the greatest risk to reliability. The Enforcement department performs its responsibilities by:

- Monitoring Regional Entities' enforcement processes and providing oversight of their outcomes to ensure due process, to identify best practices and process efficiency opportunities, and to promote consistency among Regional Entities' business practices;
- Collecting and analyzing enforcement data and trends to assist with the identification of emerging risks and to help inform the development of enforcement policies and processes;
- Filing Notices of Penalty (NOPs) and other submittals associated with noncompliance discovered through Regional Entity compliance monitoring and enforcement activities;
- Processing and filing NOPs and other submittals associated with violations discovered through NERC-led investigations and audits;
- Collaborating with other NERC departments, including Reliability Assurance, Standards, and Event Analysis,; and
- Delivering training to ERO Enterprise staff and registered entities, as well as supporting other outreach efforts.

Under §215(e)(1) of the FPA, NERC or a Regional Entity may impose a penalty on a user, owner, or operator of the BPS for a violation of a Reliability Standard approved by FERC. As the ERO, NERC has Sanction Guidelines in its ROP that govern the ERO Enterprise's determinations of penalties and non-monetary sanctions for Reliability Standard violations. The Sanction Guidelines provide information on the factors that affect penalty determinations and the behaviors, e.g., self-reporting, timely mitigation, and cooperation, that the ERO Enterprise seeks to encourage to promote compliance and reliable operations.

ERO Enterprise Core Values and Guiding Principles

The *ERO Enterprise Operating Plan* promotes the ERO Enterprise's core values and guiding principles. A goal of the ERO Enterprise is to be "a strong enforcement authority that is objective, fair, and promotes a culture of reliability excellence through risk-informed compliance monitoring, mitigation, enforcement, and registration." The following principles serve as guidelines for the conduct and behavior of all involved in the ERO Enterprise enforcement program to ensure alignment with this goal and the core values.

CEAs are independent, without conflict of interest, objective, and fair. The ERO Enterprise strives to be a strong enforcement authority that is independent, without conflict of interest, objective, and fair. NERC and each of the Regional Entities has a code of conduct addressing the professional and ethical standards applicable to its personnel. Foremost among these standards is the requirement that no person work on a matter where that work may affect the person's financial interest. The ERO Enterprise also expects its personnel to conduct themselves professionally and respectfully when engaging with registered entities or other stakeholders. Personnel who do not meet these standards are subject to discipline, up to and including termination.

The Enforcement program promotes a culture of reliability excellence through a risk-based approach. The ERO Enterprise's risk-based enforcement philosophy generally advocates reserving enforcement actions under section 5.0 of the CMEP for those issues that pose a higher risk to the reliability of the BPS. The risk of a noncompliance is determined based on specific facts and circumstances, including any controls in place at the time of the noncompliance. The ERO Enterprise works with registered entities to ensure timely remediation of potential risks to reliability and prevent recurrence of noncompliance. The enforcement process allows parties to address risks collaboratively and promote increased compliance and reliability through improvement of programs and controls at the registered entities.

The ERO Enterprise applies a presumption of non-enforcement treatment of minimal risk noncompliance to entities with demonstrated internal controls who are permitted to self-log such minimal risk issues. Regarding other issues posing a minimal risk, NERC and the Regional Entities may exercise appropriate judgment whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes. The availability of streamlined treatment of minimal risk noncompliance outside of the formal enforcement process encourages self-inspection by registered entities. When self-identified minimal risk noncompliance is more than likely not going to be subject to a financial penalty, registered entities are encouraged to establish more robust internal controls for the detection and correction of noncompliance. This approach allows the ERO Enterprise to oversee the activities of registered entities in a more efficient manner and to focus resources where they result in the greatest benefit to reliability. In this context, efficiency does not necessarily mean less time or effort. Rather, it is using the requisite time, knowledge, and skills required for each circumstance. In addition, this approach allows the ERO Enterprise to continue to provide clear signals to registered entities about identified areas of concern and risk prioritization, while maintaining existing visibility into potential noncompliance and emerging areas of risk. Outcomes for noncompliance are based on the risk of a specific noncompliance and may range from streamlined, non-enforcement processes, to significant monetary penalties.

Enforcement actions are used and penalties are imposed when warranted, commensurate with risk. An element of a risk-based approach to enforcement is accountability of registered entities for their noncompliance. No matter the risk of the noncompliance, the registered entity still bears the responsibility of mitigating that noncompliance. Based on the risk, facts, and circumstances associated with that noncompliance, the Regional Entity decides on an appropriate disposition track, inside or outside of an enforcement action, as described above, and whether a penalty is appropriate for the noncompliance.

Penalties are generally warranted for serious risk violations (e.g., uncontrolled loss of load, CIP program failures) and for when repeated noncompliance constitutes an aggravating factor. In addition to the use of significant penalties to deter undesired behavior, the ERO Enterprise also incents desired behaviors.[25]

[25] As required by §215(e)(6) of the Federal Power Act and the Commission's regulations at 18 C.F.R. §39.7(g), the Sanction Guidelines, Appendix 4B to the NERC ROP, provide that penalties and sanctions imposed for the violation of a Reliability Standard shall bear a reasonable relation to the seriousness of the violation while also reflecting consideration of the other factors specified in the Sanction Guidelines. The Sanction Guidelines are available on NERC's website.

Specifically, Regional Entities may offset penalties to encourage valued behavior. Factors that may mitigate penalty amounts include registered entity cooperation, accountability (including admission of violations), culture of compliance, and self-identification of noncompliance. Regional Entities may also grant credit in enforcement determinations for certain actions undertaken by registered entities for improvements in addition to mitigating factors. For example, Regional Entities may consider significant investments in reliability made by registered entities, beyond those otherwise planned and required, as an offset for proposed penalties in enforcement determinations. Regional Entities do not award credits or offsets for actions or investments undertaken by a registered entity that are required to mitigate noncompliance.

NERC engages in regular oversight of Regional Entity enforcement activities to confirm that the Regional Entities have followed the CMEP. This oversight evaluates the consistency of disposition methods, including assessment of a penalty or sanction, with previous resolutions of similar noncompliance involving similar circumstances. The Board Compliance Committee considers the recommendations of NERC staff regarding approval of Full NOPs and monitors the handling of noncompliance through the streamlined disposition methods of Spreadsheet NOPs, Find, Fix, Track, and Reports (FFTs), and Compliance Exceptions (CEs).

Actions are timely and transparent. NERC's ROP (including the CMEP and Sanction Guidelines) and program documents are available to the public.[26] NERC also posts information on enforcement actions on a monthly basis.[27] Moreover, information on the efficiency of the enforcement program is available to regulators, industry stakeholders, and the public on a quarterly basis.[28]

Noncompliance information is used as an input to other processes. When developing risk elements, NERC annually identifies and prioritizes risks to BPS reliability, taking into account factors such as compliance findings, event analysis experiences, and data analysis. In addition, Regional Entities consider factors such as noncompliance information when conducting an IRA of a registered entity. The ERO Enterprise also uses noncompliance information in a feedback loop to the standards development process. This allows enhanced Reliability Standards through appropriate information flows from compliance monitoring and enforcement to the standards drafting process and other NERC programs. NERC regularly provides analysis and lessons learned from noncompliance information to industry stakeholders and the public.[29]

Stakeholder Engagement and Benefit

Over the past few years, NERC and the Regional Entities have made substantial progress in reducing the number of instances of noncompliance remaining to be evaluated and processed. The ERO Enterprise has held registered entities accountable for instances of noncompliance that posed a risk to reliability while ensuring that enforcement actions are timely and transparent. NERC promotes a culture of reliability excellence by examining registered entities' internal compliance programs and considering them as mitigating factors in penalty determinations.

[26] NERC Rules of Procedure

[27] Posted compliance exceptions, Spreadsheet Notices of Penalty, and Full Notices of Penalty

[28] The CMEP reports can be found in the Compliance Committee meeting agenda packages on the Compliance Committee website.

[29] Id.

Key Efforts Underway

Enforcement Metrics

In an effort to improve the efficiency of enforcement processing throughout the ERO Enterprise, NERC developed a series of key enforcement metrics, which are tracked and analyzed throughout the year. The ERO Enterprise has continued to promote timely mitigation of noncompliance with over 99 percent of noncompliance discovered before 2015, and over 85 percent discovered in 2016, having completed Mitigation Plans or mitigating activities, reducing risk to the BPS. Including noncompliance discovered in 2017, there are 1,530 instances of noncompliance with outstanding mitigation activities. Of these, only one minimal risk instance of noncompliance has a discovery date of 2014 or earlier. It has an expected completion date in Q4 2018.

The ongoing use of CEs throughout the ERO Enterprise, has contributed to the noncompliance average age of 8.0 months. As a comparison, the average age of noncompliance was 12 months at its highest point in 2014. In 2016, it had dropped to 10.8 months. As of the end of 2017, 82 percent of the ERO Enterprise noncompliance inventory was less than one year old and only three percent was over two years old. During 2017, the ERO completed processing of all pre-2014 non-federal entity noncompliances and all but three outstanding pre-2014 federal entity noncompliances.

Continued Outreach Efforts in 2018 and Beyond

In 2018, NERC and the Regional Entities continue to conduct outreach activities that focus on self-logging, compliance exceptions, and risk assessment of noncompliance. NERC plans to use existing industry events, such as the standards and compliance workshops and industry webinars, to provide information on enforcement activities.

NERC Oversight of Risk-Based CMEP Implementation

For 2018, ensuring the successful implementation of NERC's risk-based CMEP remains the priority of Enforcement's oversight plan for the Regional Entities. As part of that oversight and in addition to offering regular feedback to the Regional Entities, NERC will continue to identify areas for improvement or promoting consistency through training, guidance, or adjustment the following year. NERC also produces an ERO Enterprise CMEP annual report, which includes an assessment of the risk-based CMEP implementation. NERC expects to publish that report during Q1 2019.

NERC performs oversight of the Regional Entities' enforcement programs primarily through the review of the processes, supporting evidence, and other information provided by the Regional Entities over the course of focused engagements of program areas that are scheduled throughout the year. NERC communicates the recommendations and findings to the Regional Entities to help the ERO Enterprise develop responsive strategies and solutions to potential issues and ensure consistent implementation of the CMEP. Such recommendations and findings also help identify priorities for training of ERO Enterprise staff during the year.

Regional Entity Training

NERC Enforcement will provide training to Regional Entity staff on the most important elements of risk-based enforcement, including risk assessment of noncompliance and the determination of appropriate penalties and sanctions for noncompliance. NERC is developing this training based on observations from its oversight activities of Regional Entity settlement agreements, as well as the process reviews described above.

CMEP Technology Project

Beginning in 2017 through 2020, NERC, in collaboration with the Regional Entities, will develop and implement a common CMEP tool that supports the CMEP, including the various processes and activities (e.g., analysis of risk, development of implementation plans and audit schedules, actual compliance monitoring, and enforcement processing). For more information on the CMEP Technology Project, see the *Information Technology* section of Section A, as well as *Exhibit F – CMEP Technology Project Business Case*.

2019 Goals and Deliverables

Specific 2019 objectives for the Enforcement department include:

- Continuing to refine and improve the risk-based CMEP processes;
- Continuing to implement in a transparent manner an ERO Enterprise enforcement philosophy that is risk-focused and drives desired behaviors by registered entities;
- Expanding the feedback loop of information from Enforcement to Standards and other program areas; and
- Working closely with NERC's Compliance Assurance and IT departments, as well as the Regional Entities, to develop application business requirements and test business functionality for the CMEP tool.

Resource Requirements

Personnel

No change in FTEs in 2019 from the 2018 budget.

Consultants and Contracts

No consultant or contract expenses are budgeted in Enforcement in 2019, which is consistent with the 2018 budget.

Other Costs

The $884k budgeted for computer and software capital expenditures is attributed to the CMEP Technology Project, for which the total capital expenditure of approximately $1.8M is split evenly between Compliance Assurance and Compliance Enforcement. The $280k increase in office costs is primarily for license and hosting fees for the new CMEP tool.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
COMPLIANCE ENFORCEMENT

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 6,608,973	$ 6,608,973	$ -	$ 6,531,811	$ (77,162)
Assessment Stabilization Reserve - Penalties	56,522	56,522	-	-	(56,522)
Total NERC Funding	**$ 6,665,495**	**$ 6,665,495**	**$ -**	**$ 6,531,811**	**$ (133,683)**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	8,444	6,333	(2,111)	15,810	7,366
Miscellaneous	-	-	-	-	-
Total Funding	**$ 6,673,939**	**$ 6,671,828**	**$ (2,111)**	**$ 6,547,621**	**$ (126,317)**
Expenses					
Personnel Expenses					
Salaries	$ 1,792,112	$ 1,935,448	$ 143,336	$ 2,006,823	$ 214,711
Payroll Taxes	115,916	117,401	1,485	125,496	9,580
Benefits	168,533	184,487	15,953	196,772	28,238
Retirement Costs	200,403	233,018	32,616	219,938	19,536
Total Personnel Expenses	**$ 2,276,963**	**$ 2,470,353**	**$ 193,390**	**$ 2,549,028**	**$ 272,065**
Meeting Expenses					
Meetings	$ 2,000	$ 2,000	$ -	$ 2,000	$ -
Travel	47,500	44,852	(2,648)	47,500	-
Conference Calls	-	1,490	1,490	2,400	2,400
Total Meeting Expenses	**$ 49,500**	**$ 48,342**	**$ (1,158)**	**$ 51,900**	**$ 2,400**
Operating Expenses					
Consultants & Contracts	$ -	$ -	$ -	$ -	$ -
Office Rent	-	-	-	-	-
Office Costs	19,160	17,729	(1,430)	299,250	280,090
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	105,014	105,014	-	105,014	-
Total Operating Expenses	**$ 124,674**	**$ 123,243**	**$ (1,430)**	**$ 404,764**	**$ 280,090**
Total Direct Expenses	**$ 2,451,137**	**$ 2,641,939**	**$ 190,802**	**$ 3,005,692**	**$ 554,555**
Indirect Expenses	**$ 2,733,948**	**$ 2,848,382**	**$ 114,434**	**$ 2,871,686**	**$ 137,738**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 5,185,085**	**$ 5,490,321**	**$ 305,236**	**$ 5,877,378**	**$ 692,293**
Change in Assets	**$ 1,488,854**	**$ 1,181,507**	**$ (307,347)**	**$ 670,243**	**$ (818,610)**
Fixed Assets					
Depreciation	$ (105,014)	$ (105,014)	$ -	$ (105,014)	$ -
Computer & Software CapEx	1,548,000	1,548,000	-	884,000	(664,000)
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	45,868	46,621	754	(108,743)	(154,610)
Inc(Dec) in Fixed Assets (B)	**$ 1,488,854**	**$ 1,489,607**	**$ 754**	**$ 670,243**	**$ (818,610)**
TOTAL BUDGET (=A+B)	**$ 6,673,939**	**$ 6,979,928**	**$ 305,990**	**$ 6,547,621**	**$ (126,317)**
FTEs	**12.22**	**11.66**	**(0.56)**	**12.22**	**-**

Reliability Assessment and System Analysis

Reliability Assessment and System Analysis (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	14.10	15.04	0.94
Direct Expenses	$ 4,256,247	$ 4,819,608	$ 563,361
Indirect Expenses	3,154,555	3,534,383	379,827
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	(97,847)	(359,212)	(261,365)
TOTAL BUDGET	$ 7,312,956	$ 7,994,779	$ 681,823

Background and Scope

The NERC Reliability Assessment and System Analysis (RASA) department, which includes the Reliability Assessment, System Analysis, and Advanced Analytics and Modeling (AAM) groups, carries out the ERO's statutory responsibility to conduct assessments of the reliability of the BPS. These assessments are used to provide insight and guidance about reliability risks, which provide a foundation for the development of new Reliability Standards or modifications to Reliability Standards, or other initiatives, such as guidelines, alert(s), webinars, etc., all focused on enhancing overall reliability. The majority of the activities in the RASA department directly address the risk priorities established by the RISC. In particular, the risks pertaining to changing resources and planning noted in the RISC report are of particular importance to the assessment and analysis work being performed in RASA.

NERC staff works closely with stakeholders on creating assessment development schedules, including schedules with adequate stakeholder review at every level. All NERC reliability assessments typically have a sponsoring technical committee, subcommittee, or other subgroup. The long-term and seasonal assessments are conducted by the NERC Planning Committee's (PC's) Reliability Assessment Subcommittee (RAS), and ultimately endorsed by the PC. Special assessments often require a separate and specialized task force or advisory group to help construct, conduct, and produce special topic assessments.

The department focuses on developing a technical framework and understanding the emerging reliability risks facing the industry. It also provides guidance and insights to stakeholders across North America. The department relies on its own engineering and analysis expertise, as well as Regional Entity and stakeholder resources. RASA is responsible for:

- Independent reliability assessments on the overall reliability and adequacy of the BES and associated emerging reliability risks that could impact the short-, mid- and the long-term (e.g., 10-year) planning horizons, and other reliability issues requiring an in-depth analysis.
- Support for the development and improvement of long-term, sustainable interconnection-based power flow, dynamic, and load models that exhibit the accuracy and fidelity reflecting actual BES reliability performance and dynamic conditions.
- Interconnection-wide analysis of steady-state and dynamic conditions, including frequency, ERS, stability, short circuit ratio, and oscillatory behavior aspects.
- Advancement of industry and the ERO's understanding of power system characteristics and behaviors by gathering larger phasor measurement units (PMU) datasets for advanced data analytics and modeling improvements.

- Assurance oversight that the BES electrical elements necessary for its reliable operation are identified, requiring the elements to follow the Reliability Standards.
- Establishment of reliability leadership and consistent, technically sound insights and recommendations that position industry and policymakers to enhance reliability through effective outreach and communications.

Stakeholder Engagement and Benefit

RASA works with industry leaders to create a reliability strategy that is relevant, timely, and effective to address the most important reliability risks. This effort includes (1) reviewing and addressing key priority risks identified by the RISC; (2) synthesizing key information identified through analysis and assessment efforts; (3) extracting and prioritizing the associated reliability risks; (4) sharing and integrating risk analysis insights across the ERO Enterprise; and (5) translating that knowledge into actionable guidance and recommendations for NERC management, the Board, and industry, along with state, federal, and provincial policymakers.

Key Efforts Underway

RASA focuses its efforts in the following key areas:

Reliability Assessment

Reliability assessments serve to evaluate the expected reliability of the BES through extensive deterministic and probabilistic analyses to identify potential reliability risks and potential mitigation approaches. These reviews include both evaluations at the edge of the planning horizon, as well as assessments of the anticipated performance during the short-term (12- to 18-month outlook). These analyses involve planned and anticipated changes to generation resources, transmission infrastructure, and load behavior compared to base-line needs of the system to remain reliable, and formulate recommendations and related guidance. This assessment is often completed by examining special scenarios and unique situations within the BES. These analyses provide a technical platform for important policy discussions on challenges facing the interconnected BES, as well as focused recommendations on mitigation to improve overall reliability or lessen reliability risks.

By identifying and quantifying emerging issues, NERC is able to provide risk-informed recommendations and support a learning environment for industry to address emerging risks and pursue improved reliability performance. These efforts are expanding to assess reliability impacts from the changing resource mix, reliability behavior of resources, distributed energy resources, and loads. Many recent resource additions are asynchronous and energy-limited, requiring assessment of a substantial number of scenarios rather than just seasonal peak conditions. Reliability assessments must therefore include a greater focus on probabilistic approaches, assessing the sufficiency of essential reliability services (ERS), as well as focusing seasonal assessments on short-term horizons to encompass evaluations beyond peak condition reserve margin analyses. Key assessments include:

- Long-Term Reliability Assessment (LTRA) (supplemented by the Probabilistic Assessment)
- Summer and Winter Reliability Assessments
- Special Reliability Assessments (selected based on high-priority/high-risk issues that require an independent assessment from the ERO)

A significant ongoing effort involving RASA, Regional Entity staff, and stakeholders focuses on effective ERS. These efforts are expected to lead to a broad set of recommendations that will culminate with defined elements, an evaluation of initial metrics and data compilation of actual performance, and refinement of the ongoing assessment of ERS measures.

As part of reliability assessment activities, NERC collects, maintains, and annually publishes the Electricity Supply and Demand (ES&D) database, which includes 10-year projections for the North American BPS. Data is validated by the Regional Entities, NERC staff, and the RAS during NERC's annual development of the LTRA. The data collection and management of its systems are an essential component to NERC's MOU with the DOE's Energy Information Agency.

System Analysis

Understanding the technical behavior of the North American grid is the foundation for identifying crucial aspects of performance that are important for sustaining overall reliability. NERC's understanding of grid behavior is achieved through constant observation and study, analytic simulations, and forensic analysis of system disturbances. The System Analysis group focuses on:

- **Power system analysis** – Develop technical analyses in key reliability areas, resulting in technically accurate and comprehensive reports addressing areas of concern (e.g., frequency response, short circuit strength, inter-area oscillation, distributed energy resources, etc.). The purpose of these technical analyses are to understand and evaluate BPS characteristics, behavior, and performance due to the changing resource mix and integration of new technology. These analyses are also intended to provide oversight, guidance, direction, and technical expertise to address key planning-related issues and interconnection-wide concerns.
- **Advance software capabilities** – Continue to explore the use of state-of-the-art software to conduct power system analysis. Enhance the usage of real-time tools used by the industry to sharpen and fine-tune models as the system evolves with the integration of new technology.
- **Technical support, implementation and outreach** – Provide technical expertise, research, and feedback to the industry. Provide foundational technical efforts that support development of key reliability planning-related standards. Solicit industry's help by using resources and leveraging any research that has been done by the industry. NERC system analysis assessment and studies are coordinated through the PC's System Analysis and Modeling Subcommittee (SAMS) in a collaborative manner to engage stakeholder involvement and support.

System analysis activities also support the following objectives:

- Continue leading and improving NERC's analytical capabilities to address a broad range of engineering topics.
- Conduct analyses and assessments in response to FERC directives.
- Support Reliability Standards development with subject matter expertise.
- Support and lead technical analysis of emerging risks requiring advanced analytics and interconnection-wide assessment.
- Conduct detailed forensic analyses of significant system disturbances.

Key focus areas include:

- PMU measurement, use, and analysis improvements
  - Synchrophasor technology
  - Power plant model verification
  - Oscillation analysis
- Frequency response analysis, interconnection frequency response obligation analysis, and forward-looking reliability assessment
- Interconnection-wide system inertia study
- Interconnection-wide short circuit ratio assessment
- Interconnection-wide model building designation and criteria administration
- Interconnection-wide model validation
- Improving model quality and fidelity
- Analysis of TPL Footnote 12
- Load and distributed energy resource modeling
- Event analysis (simulation and forensic analysis of major events)
- Reliability Standards support
- BES exception and self-determined notification processing

Advanced Analytics and Modeling

The AAM group focuses on emerging reliability risks to the BPS through advanced system analysis techniques and modeling capabilities. The AAM group works collaboratively with NERC stakeholders, particularly through the NERC PC and Operating Committee (OC) as well as their technical subgroups. Through these activities, AAM's key focuses include:

- **State of Modeling Report** – Provide industry insight related to modeling improvements and interconnection-wide system analysis, with recommendations for enhancement and industry engagement. Provide industry with annual updates related on modeling and modeling practices.
- **Inverter-based resource performance** – Perform event analyses and investigate abnormal performance of inverter-based resources, particularly solar photovoltaic. Develop industry recommendations and address potential reliability gaps through NERC Alerts, guidelines, technical reference documents, industry education, and evaluation of Reliability Standards. Coordinate the PC's Inverter-Based Resource Performance Task Force (IRPTF).
- **Distributed energy resources** – Support industry in the reliable integration of increased levels of distributed energy resources. Provide industry leadership and technical guidance on key reliability impacts of distributed energy resources. Develop recommended practices (modeling, planning, and operations) to ensure BPS reliability.
- **Synchrophasor technology** – Support industry adoption and advancement of synchrophasor technology through the PC's Synchronized Measurement Subcommittee (SMS). Study interconnection-wide oscillatory behavior (and other interconnection-wide phenomena) through PMU data collected from RCs.
- **Power plant model verification** – Support industry understanding and expertise in power plant modeling through the PC's System Analysis and Modeling Subcommittee's (SAMS's) Power Plant Modeling and Verification Task Force (PPMVTF). Advance capabilities to perform a disturbance-based model verification, working with software vendors. Support industry implementation of MOD-026-1 and MOD-027-1.

- **Dynamic load modeling** – Drive improvements of dynamic load modeling capabilities in support of industry stability studies for planning and real-time reliability assessments. Advance state of the art modeling capability across North America. Support the SAMS's Load Modeling Task Force (LMTF) efforts.
- **Changing end-use loads** – Support studies and technical positions on the changing nature of end-use loads and advocate for grid-friendly load behavior. Engage with industries collaboratively, working with utility members, to represent BPS needs.
- **Interconnection-wide case quality assessments** – Perform annual assessments of case quality and fidelity on the interconnection-wide cases released by the MOD-032 designees. Develop a feedback loop mechanism with the MOD-032 designees to instigate improvements to models.
- **Modeling notifications** – Proactively address deficiencies in interconnection-wide models and provide industry education on key modeling topics as identified by NERC or industry.
- **Interconnection Reliability Operating Limits** (IROLs) – Coordinate with the PC's Methods for Establishing IROLs Task Force (MEITF) and support improvements to the methods, practices, and tools used for establishing IROLs. Coordinate with industry and FERC on potential new approaches to characterize IROLs while ensuring reliable operation of the BPS.

Technical Committees

RASA coordinates and administers the activities and efforts of the PC and its subgroups. The PC and its subgroups provide the oversight, guidance, and leadership essential to address these areas of strategic focus efficiently and comprehensively, and ensure technical accuracy, with the objective of enhancing BPS reliability. Further, the PC recognizes the need to strengthen the ties between the technical committees to ensure expertise is leveraged and amplified, thereby increasing the relevance and value of the technical committee results. NERC supports industry volunteers and helps them achieve industry consensus around important and strategic reliability issues as identified by the RISC and detailed in the *ERO Enterprise Long-Term Strategy* and *ERO Enterprise Operating Plan*.

NERC and Regional Entity Coordination

NERC's Reliability Assessment and Performance Analysis (RAPA) staff coordinate with Regional Entity counterparts through the ERO RAPA Group to collaborate on and provide oversight for reliability assessment and reliability risk analysis functions. The responsibilities of this group include facilitating the exchange of information, jointly coordinating work product expectations (scope, timing, schedule, resource expenditures, budget assumptions, etc.), and promoting consistency across the ERO Enterprise. Additionally, ERO RAPA continually seeks improvements to data and information coordination, methods, and approaches for the advancement of BPS risk analysis, and interfaces with the NERC technical committees accordingly to fulfill these objectives. Key objectives include:

- Program management and operations
  - Achieve consistent implementation and alignment across the ERO Enterprise for reliability assessment and performance analysis functions.
  - Periodically review coordination plans and ensure they are aligned with the *ERO Enterprise Operating Plan.*
- Program oversight
  - Provide oversight to reliability assessments and other key reports. ERO RAPA establishes common approaches and processes for reliability assessments and solutions for program challenges.

  - Implement enhancements to improve ERO Enterprise-wide efficiency and effectiveness of RAPA-related functions.

- Data and information coordination
  - Provide consistent oversight materials regarding data collection, checking, validation, and assessment for use throughout NERC and the Regional Entities.
  - Coordinate data and information systems across the ERO Enterprise.

Further, RASA continues to work closely with other organizations, including but not limited to the Electric Power Research Institute (EPRI), the DOE, the Institute of Electrical and Electronic Engineers (IEEE), the Institute of Nuclear Power Operations (INPO), the North American Transmission Forum (NATF), the North American Generation Forum (NAGF), and the Canadian Electricity Association (CEA). RASA collaborates with these groups on a number of fronts, including GMD, vegetation management, and variable generation integration. RASA also works with the Interstate Natural Gas Association of America (INGAA) and the Natural Gas Supply Association (NGSA) regarding studies pertaining to the interdependency of gas and electric systems.

2019 Goals and Deliverables

RASA activities and deliverables for 2019 are in support of the following goals and objectives identified in the *ERO Enterprise Operating Plan*.

Goal 3: Reduction of Known Risks to Reliability

- Ensure that the IRPTF completes its scope of work on schedule and implements the recommendations needed to maintain reliability. The recommendations should include addressing any gaps in Reliability Standards.
- Collaborate with Planning Coordinators to expand development of interconnection-wide models with expected dispatches to support effective long-term planning assessments.
- Work with stakeholders to develop and share knowledge and information supporting BPS resilience.

Goal 4: Identification and Assessment of Emerging Reliability Risks

- Improve resource adequacy assessments with increased probabilistic and risk analysis.
- Conduct interconnection-wide analysis of steady-state and dynamic conditions, including frequency, ERS, stability, short circuit ratio, and oscillatory behavior aspects to support NERC's reliability assessments and improve industry planning.
- Perform model validations at the interconnection level and compare with internal transmission owner models (short circuit model validation).
- Gather additional system performance data (e.g., data on balancing and frequency performance, renewables, and ERS) to advance analytics and improve modeling.
- Increase technical analysis and assessment focus on natural gas, wind, and solar resource and fuel availability.
- Develop technical references and guidelines that advance and improve reliability using new technologies.
- Develop quality and fidelity assessments of interconnection models.

Resource Requirements

Personnel

The increase of one position (0.94 FTEs) is the result of resource allocations to realign staff with current needs.

Consultants and Contracts

The total consultant and contract expenses for the RASA department increased from $525k in 2018 to $625k in 2019, specifically to support research on the reliability effects of GMD. A detailed breakdown of 2018 and 2019 budgeted expenses are shown in *Exhibit B – Consultant and Contract Costs*.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
RELIABILITY ASSESSMENT and SYSTEM ANALYSIS

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 7,212,995	$ 7,212,995	$ -	$ 7,950,320	$ 737,325
Assessment Stabilization Reserve - Penalties	65,217	65,217	-	-	(65,217)
Total NERC Funding	**$ 7,278,213**	**$ 7,278,213**	**$ -**	**$ 7,950,320**	**$ 672,108**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	25,000	25,000	-	25,000	-
Interest	9,743	7,307	(2,436)	19,459	9,716
Miscellaneous	-	-	-	-	-
Total Funding	**$ 7,312,956**	**$ 7,310,520**	**$ (2,436)**	**$ 7,994,779**	**$ 681,823**
Expenses					
Personnel Expenses					
Salaries	$ 2,334,967	$ 2,481,288	$ 146,321	$ 2,589,488	$ 254,522
Payroll Taxes	144,330	152,640	8,309	157,593	13,262
Benefits	283,513	319,146	35,633	343,858	60,345
Retirement Costs	258,277	304,373	46,096	282,584	24,307
Total Personnel Expenses	**$ 3,021,087**	**$ 3,257,446**	**$ 236,359**	**$ 3,373,524**	**$ 352,437**
Meeting Expenses					
Meetings	$ 121,000	$ 121,000	$ -	$ 121,000	$ -
Travel	250,000	249,800	(200)	250,000	-
Conference Calls	-	1,490	1,490	6,500	6,500
Total Meeting Expenses	**$ 371,000**	**$ 372,290**	**$ 1,290**	**$ 377,500**	**$ 6,500**
Operating Expenses					
Consultants & Contracts	$ 525,000	$ 525,000	$ -	$ 625,000	$ 100,000
Office Rent	-	-	-	-	-
Office Costs	187,889	207,207	19,318	217,710	29,821
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	150,771	150,771	-	225,375	74,604
Total Operating Expenses	**$ 864,160**	**$ 883,478**	**$ 19,318**	**$ 1,068,585**	**$ 204,425**
Total Direct Expenses	**$ 4,256,247**	**$ 4,513,214**	**$ 256,967**	**$ 4,819,608**	**$ 563,361**
Indirect Expenses	**$ 3,154,555**	**$ 3,581,242**	**$ 426,687**	**$ 3,534,383**	**$ 379,827**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 7,410,803**	**$ 8,094,457**	**$ 683,654**	**$ 8,353,991**	**$ 943,188**
Change in Assets	**$ (97,847)**	**$ (783,937)**	**$ (686,090)**	**$ (359,212)**	**$ (261,365)**
Fixed Assets					
Depreciation	$ (150,771)	$ (150,771)	$ -	$ (225,375)	$ (74,604)
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	52,924	58,616	5,692	(133,837)	(186,761)
Inc(Dec) in Fixed Assets (B)	**$ (97,847)**	**$ (92,155)**	**$ 5,692**	**$ (359,212)**	**$ (261,365)**
TOTAL BUDGET (=A+B)	**$ 7,312,956**	**$ 8,002,302**	**$ 689,346**	**$ 7,994,779**	**$ 681,823**
FTEs	**14.10**	**14.66**	**0.56**	**15.04**	**0.94**

Reliability Risk Management

NERC's Reliability Risk Management (RRM) department carries out the ERO's statutory responsibility to perform assessments (real-time or near real-time continual awareness, detailed analysis of significant events, and longer-term broad performance assessments) of the reliability and adequacy of the BPS including identifying potential issues of concern relating to system, equipment, entity, and human performance that may indicate the need to implement targeted interventions. RRM has three groups: Situation Awareness (also referred to as Bulk Power System Awareness), Event Analysis, and Performance Analysis. These groups have six primary functions: (1) BPS awareness; (2) event and root cause analysis; (3) assessment of human performance challenges that affect reliability and identification of improvement opportunities; (4) continent-wide analysis and reporting of BPS performance; and (5) support of the OC.

RRM's functions and resources are directly focused on proactive awareness of BPS conditions and all events over a threshold of certain risk or impact. Through awareness and continuous assessment, RRM identifies potential reliability risks. RRM analyzes events in detail, addresses the most significant risks to reliability, and ensures that industry is well informed of system events, emerging trends, risk analysis, and lessons learned. Through performing these functions, RRM provides data and analysis to inform other aspects of NERC's statutory functions. The group also provides strategic direction for using risk-based concepts in planning and executing its responsibilities.

Situation Awareness

Situation Awareness (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	5.64	5.64	-
Direct Expenses	$ 2,566,215	$ 2,604,063	$ 37,847
Indirect Expenses	1,261,822	1,325,394	63,571
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	18,610	340,863	322,253
TOTAL BUDGET	$ 3,846,648	$ 4,270,319	$ 423,672

Background and Scope

NERC's Situation Awareness group and the Regional Entities monitor BPS conditions, significant occurrences and emerging risks, and threats across the 14 RC regions in North America to maintain an understanding of conditions and situations that could impact reliable operation. This group also supports the development and publication of NERC Alerts and awareness products and facilitates information sharing among industry, the Regional Entities, and the government during crisis situations and major system disturbances. The process for understanding the potential threats or vulnerabilities to BPS reliability starts with understanding occurrences and events in the context in which they occur.

Stakeholder Engagement and Benefit

BPS conditions continually change and provide recognizable signatures through automated tools, mandatory reports and voluntary information sharing, and third-party publicly available sources. The significant majority of these signatures represents conditions and occurrences that have little or no reliability impact, either positive or adverse, on the BPS. However, being cognizant of the short-term condition of the BPS and the signatures associated with the entire range of reliability performance helps the ERO identify significant occurrences more accurately and efficiently. Registered entities continue to robustly share information and collaborate with the ERO to maintain and improve the overall reliability.

Key Efforts Underway

Situation Awareness focuses on the following in support of the *ERO Enterprise Operating Plan*:

- Ensure that the ERO is aware of all BES events above a threshold of impact.
- Enable the sharing of information and data to facilitate wide-area situational awareness.
- During crisis situations, facilitate the exchange of information among industry, the Regional Entities, and the U.S. and Canadian governments.
- Keep industry informed of emerging reliability threats and risks, including any expected actions.
- Conduct the annual NERC Monitoring and Situational Awareness Conference and Human Performance Conference.
- Administer the NERC Alerts process as specified in ROP §810 to issue Advisory (Level 1) Alerts on significant and emerging reliability- and security-related topics as needed, and facilitate the tracking of actions specified in Recommendation (Level 2) and Essential Action (Level 3) Alerts.
- Perform oversight, as per the Situation Awareness Oversight Plan, of the activities and performance of the Regional Entities.

The department uses the following major reliability-related tools to support department activities:

- **Resource Adequacy (Area Control Error [ACE] Frequency) Tool –** This software application provides continuous monitoring of key resource adequacy performance metrics, including pre-established thresholds and limits defined in standards. It alerts RCs and resource subcommittees to conditions that could result in critical inadequacies, such as major tie errors, inaccurate load forecasts, and inadequate frequency response.
- **Inadvertent Interchange** – This tool facilitates the entering of monthly scheduling data and submittal of monthly inadvertent performance standards reports to NERC. It also assists in the monitoring and resolution of reliability issues originated by inadvertent interchange imbalances.
- **Frequency Monitoring and Analysis Tool –** This tool detects frequency events and captures key frequency response information for each interconnection.
- **Intelligent Alarms Tool** – This tool detects short-term and long-term frequency deviations using data transmitted to NERC by the BAs. When coupled with the FNet[30] and Frequency Monitoring and Analysis tools, this tool allows immediate differentiation of the cause of a frequency deviation—a generator trip or a scheduling error.
- **Genscape** – The PowerIQ and PowerRT tools provide more detailed insight into current-day conditions impacting BPS conditions in both normal operations and stressed conditions.
- **Process Information (PI) Historian System** – The PI Historian system benefits RASA for the attainment of deliverables recommended in the 2015 ERS Task Force (ERSTF) Report (specifically, collect and analyze system inertia data) and offers longer term value for both RASA and RRM. The system enables the continued strategy to transition away from other applications, offsetting future expenses by replicating the functionality of Resource Adequacy and Intelligent Alarms in-house in the 18–36 months outlook, and creates the necessary foundation for NERC's eventual receipt and consumption of streaming synchrophasor data in near real time.

[30] FNet – Operated by the Power Information Technology Laboratory at the University of Tennessee, FNet is a low-cost, quickly deployable global positioning system (GPS)-synchronized wide-area frequency measurement network. High dynamic accuracy Frequency Disturbance Recorders are used to measure the frequency, phase angle, and voltage of the power system at ordinary 120 V outlets. The measurement data are continuously transmitted via the Internet to the FNet servers hosted at the University of Tennessee and Virginia Tech.

Several reliability-related situational awareness and monitoring tools and processes are undergoing enhancement or modification. The following are being focused on during 2018: (1) an upgrade to the SAFNR software application to include preparation of a request for proposals (RFP) in late 2018; (2) operation and maintenance of the NERC Alerts tool while planning for a streamlined NERC Alert process and platform appropriately integrated with related ongoing NERC, E-ISAC, and ERO Enterprise IT initiatives; (3) a refresh of the Reliability Coordinator Information System (RCIS) legacy application for operability and maintainability reasons, with no significant changes to functionality; and (4) continuing to set the conditions to bring limited streaming synchrophasor data into NERC for wide-area situational awareness and event triage applications.

2019 Goals and Deliverables

In 2019, the Situation Awareness group will continue to accomplish the specific goals and deliverables referenced above in support of the *ERO Enterprise Operating Plan*, and will also focus on the upgrade to the SAFNR application. The current SAFNR platform limits the Situation Awareness group's ability to accurately understand current conditions on the BPS due to the inability to easily or cost-effectively update the underlying power system information, including incorporating available real-time data feeds on risks to reliability, such as severe weather, flooding, and wildfires, as well as available information on interconnection frequency, BA ACE, and aggregated customer outages.

Further, enhancing SAFNR will incorporate functionality elements piloted during GridEx IV that will enable the Situation Awareness group to provide the E-ISAC and the ESCC with more timely and understandable common operating picture information, meeting the *GridEx IV Executive Tabletop Report* recommendation that states that NERC and the E-ISAC should enhance their ability to provide reliable, timely, and accurate information regarding the state of grid reliability and security threats and events, and largely meeting the observation #3 recommendation from the *GridEx IV Distributed Play Lessons Learned Report*, which states that the E-ISAC should consider adding a "common operational picture" function to the E-ISAC portal.

With the insight gained from more than five years of use, the system can be implemented as envisioned—a shared platform for rapid and accurate situational awareness that appropriately protects the proprietary information in the tool while maximizing the value of understanding shared to the right audiences. See *Exhibit G – Situation Awareness for FERC, NERC, and the Regional Entities (SAFNR)* for further details.

Resource Requirements

Personnel

No change in FTEs for 2019 from the 2018 budget.

Consultants and Contracts

The overall funding of approximately $1.3M for consultant and contract expenses (which largely includes support costs of the tools described above) in 2019 is consistent with the 2018 budget. A detailed breakdown of the 2018 and 2019 budgeted expenses is shown in *Exhibit B – Consultant and Contract Costs*.

Other Costs

The $400k increase for computer and software capital expenditures is attributed to the upgrade for SAFNR, for which the total capital expenditure of $600k is split between Situation Awareness and the E-ISAC.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
SITUATION AWARENESS

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 3,816,664	$ 3,816,664	$ -	$ 4,263,022	$ 446,359
Assessment Stabilization Reserve - Penalties	26,087	26,087	-	-	(26,087)
Total NERC Funding	**$ 3,842,751**	**$ 3,842,751**	**$ -**	**$ 4,263,022**	**$ 420,272**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	3,897	2,923	(974)	7,297	3,400
Miscellaneous	-	-	-	-	-
Total Funding	**$ 3,846,648**	**$ 3,845,674**	**$ (974)**	**$ 4,270,319**	**$ 423,672**
Expenses					
Personnel Expenses					
Salaries	$ 888,593	$ 759,509	$ (129,084)	$ 886,295	$ (2,299)
Payroll Taxes	59,143	52,362	(6,780)	58,745	(398)
Benefits	144,353	158,282	13,930	171,166	26,813
Retirement Costs	98,676	104,444	5,769	97,619	(1,056)
Total Personnel Expenses	**$ 1,190,764**	**$ 1,074,598**	**$ (116,166)**	**$ 1,213,825**	**$ 23,061**
Meeting Expenses					
Meetings	$ 2,000	$ 2,000	$ -	$ 2,000	$ -
Travel	33,000	26,400	(6,600)	33,000	-
Conference Calls	-	1,491	1,491	-	-
Total Meeting Expenses	**$ 35,000**	**$ 29,891**	**$ (5,109)**	**$ 35,000**	**$ -**
Operating Expenses					
Consultants & Contracts	$ 1,295,495	$ 1,295,495	$ -	$ 1,280,990	$ (14,505)
Office Rent	-	-	-	-	-
Office Costs	41,897	40,115	(1,782)	64,800	22,903
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	2,559	2,559	-	8,948	6,389
Total Operating Expenses	**$ 1,340,451**	**$ 1,338,670**	**$ (1,782)**	**$ 1,355,238**	**$ 14,787**
Total Direct Expenses	**$ 2,566,215**	**$ 2,443,159**	**$ (123,056)**	**$ 2,604,063**	**$ 37,847**
Indirect Expenses	**$ 1,261,822**	**$ 1,038,218**	**$ (223,604)**	**$ 1,325,394**	**$ 63,571**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 3,828,038**	**$ 3,481,378**	**$ (346,660)**	**$ 3,929,456**	**$ 101,419**
Change in Assets	**$ 18,610**	**$ 364,296**	**$ 345,686**	**$ 340,863**	**$ 322,253**
Fixed Assets					
Depreciation	$ (2,559)	$ (2,559)	$ -	$ (8,948)	$ (6,389)
Computer & Software CapEx	-	-	-	400,000	400,000
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	21,170	16,993	(4,176)	(50,189)	(71,359)
Inc(Dec) in Fixed Assets (B)	**$ 18,610**	**$ 14,434**	**$ (4,176)**	**$ 340,863**	**$ 322,253**
TOTAL BUDGET (=A+B)	**$ 3,846,648**	**$ 3,495,811**	**$ (350,837)**	**$ 4,270,319**	**$ 423,672**
FTEs	**5.64**	**4.25**	**(1.39)**	**5.64**	**-**

Event Analysis

Event Analysis (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	11.28	10.34	(0.94)
Direct Expenses	$ 2,680,449	$ 2,664,060	$ (16,389)
Indirect Expenses	2,523,644	2,429,888	(93,756)
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	(42,604)	(177,595)	(134,991)
TOTAL BUDGET	$ 5,161,490	$ 4,916,353	$ (245,137)

Background and Scope

The Event Analysis group performs assessments of the reliability and adequacy of the BES. This includes identifying potential issues of concern related to system, equipment, entity, and human performance that may indicate a need to develop remediation strategies, action plans, or data used to revise or retire Reliability Standards or consider new Reliability Standards. The group analyzes and determines the cause of the events, promptly ensures tracking of corrective actions to prevent recurrence, and provides lessons learned to the industry. Event Analysis ensures that reporting and analysis are consistent to allow wide-area assessment of trends and risks. The department analyzes all reportable events for sequence of events, root cause, risk to reliability, and mitigation, and keeps the industry well informed of system events, emerging trends, risk analysis, lessons learned, and expected actions.

Additional resources within this department focus on identifying human-error risks and those precursor factors that allow human error to impact system reliability. The department educates industry regarding risks, precursors, and mitigation methods. Resources also support compliance and standards training initiatives and trending and analysis to identify emerging reliability risks. These efforts are conducted in collaboration with industry human performance projects, including WECC's Human Performance Working Group, the OC's Event Analysis Subcommittee (EAS), and others.

Stakeholder Engagement and Benefit

The Event Analysis department coordinates the use of collective resources, consistency in analysis, and timely delivery of event analysis reports.[31] The ERO disseminates lessons learned and other useful information to the electric industry obtained from or as a result of event analysis. The Event Analysis team conducts in-depth analyses of approximately 150 events per year on average. Annually, the team also conducts calls facilitated by the Regional Entities with over 140 registered entities to finalize root and contributing causes for the categorized events analyzed. Major analysis to date includes continuing assessment of Energy Management System (EMS) outages, continued collaboration with the RASA and Performance Analysis groups on frequency response performance, analyses of substation equipment failure events, and protective relay trends, including ground overcurrent relay misoperations, relay communication system failures, and the importance of commissioning testing.

Collaboration with the Trade Associations and Forums

The activities of the NATF, the NAGF, trade associations, and other industry groups are expected to compliment ERO Enterprise activities and limit the need to add incremental resources to the NERC and Regional Entity BP&Bs that might otherwise be required in the absence of these forums.

[31] The core process for Event Analysis is outlined in the approved process: ERO Event Analysis Process - Version 3.1 (December 2016).

NATF has been invited to participate in several reliability initiatives that are expected to continue into 2019, including protection systems misoperations reduction, challenges associated with inverter-based resources, physical security, various activities related to reliability assurance initiatives, improvement of modeling practices, and complementary efforts on addressing the GMD challenges.

Event Analysis seeks to accomplish several specific goals and objectives as part of the strategic focus of the ERO Enterprise and in support of the *ERO Enterprise Operating Plan*:

- Work with the Regional Entities to review information from registered entities on qualifying events and disturbances advancing awareness of events above a threshold level; facilitate analysis of root and contributing causes, risks to reliability, wide-area assessments, and remediation efforts; and disseminate information regarding events in a timely manner.
- Ensure that all reportable events are analyzed for sequence of events, root cause, risk to reliability, and mitigation.
- Continue to refine risk-based methods to support better identification of reliability risks, including the use of more sophisticated cause codes for analysis.
- Conduct training (webinars, workshops, and conference support) to inform industry and the ERO Enterprise of lessons learned, root cause analysis, trends, human performance, and extreme weather preparedness and recommendations.
- Develop reliability recommendations and Alerts as needed and track industry accountability for critical reliability recommendations.
- Ensure that industry is well informed of system events, emerging trends, risk analysis, lessons learned, and expected actions.
- Conduct major event analysis and reporting of major findings and recommendations that will improve reliability.
- Perform oversight, as per the Event Analysis Oversight Plan, of the activities and performance of the Regional staffs.

The Event Analysis department also supports several of the top-priority reliability risk projects as identified and described under the Performance Analysis section of this document.

2019 Goals and Deliverables

In 2019, the Event Analysis group will continue to accomplish the specific goals and deliverables referenced above in support of the *ERO Enterprise Operating Plan*, particularly with regard to analysis in the area of inverters and inverter technologies as the proliferation of renewables using these technologies are rapidly increasing.

Resource Requirements

Personnel

The reduction in FTEs is the result of the elimination of one open position (0.94 FTEs) from the Event Analysis group.

Consultants and Contracts

No funding is budgeted for consultant and contract expenses in 2019, which is consistent with the 2018 budget.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
EVENT ANALYSIS

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 5,061,521	$ 5,061,521	$ -	$ 4,862,975	$ (198,546)
Assessment Stabilization Reserve - Penalties	52,174	52,174	-	-	(52,174)
Total NERC Funding	**$ 5,113,695**	**$ 5,113,695**	**$ -**	**$ 4,862,975**	**$ (250,720)**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	40,000	40,000	-	40,000	0
Interest	7,794	5,846	(1,949)	13,378	5,583
Miscellaneous	-	-	-	-	-
Total Funding	**$ 5,161,490**	**$ 5,159,541**	**$ (1,949)**	**$ 4,916,353**	**$ (245,137)**
Expenses					
Personnel Expenses					
Salaries	$ 1,783,120	$ 1,705,279	$ (77,842)	$ 1,749,243	$ (33,877)
Payroll Taxes	110,619	103,487	(7,132)	103,054	(7,565)
Benefits	227,802	233,705	5,903	254,624	26,822
Retirement Costs	198,179	204,137	5,957	192,057	(6,122)
Total Personnel Expenses	**$ 2,319,720**	**$ 2,246,607**	**$ (73,113)**	**$ 2,298,978**	**$ (20,742)**
Meeting Expenses					
Meetings	$ 81,500	$ 81,500	$ -	$ 81,500	$ 0
Travel	150,000	147,680	(2,320)	150,000	-
Conference Calls	-	1,737	1,737	-	-
Total Meeting Expenses	**$ 231,500**	**$ 230,918**	**$ (582)**	**$ 231,500**	**$ 0**
Operating Expenses					
Consultants & Contracts	$ -	$ -	$ -	$ -	$ -
Office Rent	-	-	-	-	-
Office Costs	43,786	58,825	15,040	47,500	3,714
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	84,943	84,943	-	85,582	639
Total Operating Expenses	**$ 129,229**	**$ 144,268**	**$ 15,040**	**$ 133,582**	**$ 4,353**
Total Direct Expenses	**$ 2,680,449**	**$ 2,621,793**	**$ (58,656)**	**$ 2,664,060**	**$ (16,389)**
Indirect Expenses	**$ 2,523,644**	**$ 2,657,839**	**$ 134,194**	**$ 2,429,888**	**$ (93,756)**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 5,204,093**	**$ 5,279,632**	**$ 75,538**	**$ 5,093,948**	**$ (110,146)**
Change in Assets	**$ (42,604)**	**$ (120,091)**	**$ (77,487)**	**$ (177,595)**	**$ (134,991)**
Fixed Assets					
Depreciation	$ (84,943)	$ (84,943)	$ -	$ (85,582)	$ (639)
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	42,339	43,502	1,163	(92,013)	(134,352)
Inc(Dec) in Fixed Assets (B)	**$ (42,604)**	**$ (41,441)**	**$ 1,163**	**$ (177,595)**	**$ (134,991)**
TOTAL BUDGET (=A+B)	**$ 5,161,490**	**$ 5,238,191**	**$ 76,702**	**$ 4,916,353**	**$ (245,137)**
FTEs	**11.28**	**10.88**	**(0.40)**	**10.34**	**(0.94)**

Performance Analysis

Performance Analysis (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	9.40	9.40	-
Direct Expenses	$ 2,639,101	$ 2,967,901	$ 328,799
Indirect Expenses	2,103,037	2,208,989	105,952
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	(108,716)	(379,643)	(270,927)
TOTAL BUDGET	$ 4,633,422	$ 4,797,247	$ 163,825

Background and Scope

The Performance Analysis department currently consists of balancing and frequency control (B&FC) and data analytics (DA) groups and provides significant statistical analysis and outreach support for NERC and the entire ERO Enterprise. The outreach includes initiatives with the Regional Entities and electricity industry-related organizations.

B&FC Scope

B&FC provides support and services necessary for the real-time operation of the BPS in the areas of balancing resources and demand, interconnection frequency, interchange scheduling, and control performance. B&FC is responsible for providing technical assistance in the development and administration of the NERC balancing standards (BAL standards) that include BAL-001 Real Power Balancing Control Performance, BAL-002 Disturbance Control Performance, BAL-003 Frequency Response and Frequency Bias Setting, BAL-004 Time Error Correction, and BAL-006 Inadvertent Interchange. B&FC is also instrumental in performing the analysis and development of annual reports and informational filings that satisfy the FERC directives set forth in the orders that approved the balancing standards.

B&FC supports the OC's Resources Subcommittee (RS), Frequency Working Group (FWG), Inadvertent Interchange Working Group (IIWG), and Reserves Working Group (RWG) through facilitation of quarterly in-person meetings, organizing and hosting of teleconferences as needed, drafting and posting of agendas and meeting minutes, and hosting subcommittee and industry webinars. B&FC also maintains the RS website and Balancing Authority Submittal Site (BASS), which are critical to industry stakeholders by providing operational information and a submittal mechanism for the aforementioned balancing standard requirements.

The PC and OC jointly created the ERS Working Group (ERSWG) to advance the work initiated by the ERSTF in consideration of the technical and operational impacts to BPS reliability that could result from the changing generation resource mix throughout North America. B&FC provides support through data collection, analysis, and reporting for five of the ERS measures that include Measure 1: Synchronous Inertial Response at an Interconnection Level, Measure 2: Initial Frequency Deviation Following Largest Contingency, Measure 3: Synchronous Inertial Response at a BA Level, Measure 4: Frequency Response at an Interconnection Level, and Measure 6: Net Demand Ramping Variability. B&FC supports the annual *State of Reliability* report (SOR report) by providing data and analysis for interconnection frequency response (M-4) and related statistical analysis.

In 2017, B&FC partnered with the Situation Awareness group, IT, and OSIsoft to accomplish the specification, development, and installation of a PI Historian system that allows NERC to retrieve, analyze, and report on data that is currently hosted and analyzed by external parties. The initial data includes

interconnection frequency and BA ACE across North America and provides enhanced wide area visualization and analysis of the North American BES. B&FC is leading the effort to build the asset framework hierarchy that will further enhance analysis and reporting that support the efforts of NERC staff and technical committees. Near-term project initiatives include the retrieval of high-speed sub-second frequency data from the University of Tennessee at Knoxville into the NERC PI Historian. While the implementation of PI Historian at NERC is a very large step forward, the maintenance of this database and continued development of visualization, analysis, and reporting tools continue to be a considerable effort and resource requirement going forward.

DA Scope

DA is responsible for the collection, management, and analysis of data related to the performance of five areas of BPS operations: transmission, conventional generation, wind generation, protection system misoperations, and demand response. DA also provides application training and end-user support to reporting entities and Regional Entity staff. DA collaborates with internal and external stakeholders through working groups associated with the industry sectors reporting performance data to define and revise reporting requirements and related applications. Analysis performed by DA includes identifying potential risks of concern related to system, equipment, entity, and organizational performance that may indicate a need to develop remediation strategies, improvements to the reporting applications, new data collection or analysis tools, or data used to create, revise, or retire reliability standards or consider new reliability standards or reporting areas. Such analysis provides the foundation for the annual SOR report, the annual misoperations report, and technical papers to the industry.

DA continues the 2018 trend of highly concentrated business engagement in IT projects. 2019 projects include: (1) the planning and subsequent deployment of the solar data collection system; (2) continued refinement and implementation of the data sharing process to comply with FERC Order 824; (3) development of portal applications on the NERC enterprise platform; (4) integration of the next application data set for the ERO data warehouse; and (5) continued planning and collection of ROP Section 1600 data requests, including but not limited to GMD studies and cyber and physical security data. Throughout these projects, DA has developed effective and efficient processes and work products that are being adopted by the NERC Project Management Office as models for other NERC IT projects. To improve data quality, DA conducts multiple multi-day in-person training sessions for end-users that provide data to the reporting applications. In addition to its legacy work with data collection and analysis, DA provides business subject matter expertise for several IT projects, including new data reporting and analytical tools, projects to support FERC data needs, ERO Enterprise data sharing, as well as projects with other NERC groups.

Stakeholder Engagement and Benefit

The Performance Analysis group monitors the performance and identifies risks to reliability of the BES in North America through analyzing data from industry measuring historic trends. The group provides reports and recommendations regarding the anticipated conditions that could impact the reliability, security, and stability of the BPS to the industry, Regional Entities, regulatory entities, and other designated entities.

Performance Analysis works with industry leaders to create a reliability strategy that is relevant, timely, and effective at addressing the most important reliability risks. This effort includes Performance Analysis's contribution (including its data gathering and statistical analyses of data, trends, and events) toward the ERO's understanding of key information identified through (1) analysis and assessment efforts; (2) extraction and prioritization of the associated reliability risks from that information; (3) communication and integration of those risk analysis insights across the ERO Enterprise; and (4) translation of that knowledge into actionable guidance and recommendations for NERC management, the Board, industry,

and state, federal, and provincial policymakers. This offers stakeholders an open and transparent approach for the development of NERC's reliability strategy, ultimately ensuring the ERO is accountable to industry, regulators, and the public at large.

B&FC will continue to support the RS, ERSWG, and industry stakeholders through performance-based webinars, technical whitepapers, reliability guidelines, and individual outreach. These efforts have proven successful throughout 2017 and 2018, with an emphasis on frequency response performance and operational capabilities.

Key Efforts Underway

In addition to support of the RS and its working groups, the maintenance and administration of the BAL standards is a major effort for B&FC, with particular current focus on BAL-003-1 Frequency Response and Frequency Bias Setting. B&FC fulfils the ongoing tasks assigned to the ERO in BAL-003-1 Attachment A and the Procedure for ERO Support. These tasks include, but are not limited to:

- Ongoing quarterly identification, review, selection, and posting of BAL-003-1 and M-4 frequency events for use by BAs and other industry stakeholders;
- Calculation and posting of Minimum Frequency Bias Settings for each BA;
- Calculation and assignment of BA Frequency Response Obligations for the upcoming year;
- Calculation and assignment of BA annual Frequency Bias Settings and L10 values for April implementation into BA control systems;
- Ongoing maintenance of and necessary modifications to BAL-003-1 Frequency Response Standard Forms used by BAs to calculate frequency response performance and document bilateral purchase or sale of frequency response and/or participation in a Frequency Response Sharing Group in accordance with BAL-003-1;
- Maintenance of the BASS used by BAs for BAL-003-1 submittals and performance of vetting for stakeholders requesting access to the BASS;
- Ongoing annual development of the Frequency Response Annual Analysis Report, which is necessary to identify changes in frequency response performance and recommend changes in Interconnection Frequency Response Obligations in accordance with BAL-003-1; and
- Leading efforts related to FERC Order 794 that approved the BAL-003-1 standard and directed NERC to submit a report in 2018 addressing (1) an evaluation of the use of linear regression methodology to calculate frequency response and (2) the availability of resources for applicable entities to meet the Frequency Response Obligation.

The key trends, findings, and recommendations from Performance Analysis serve as technical input to Reliability Standards and standards project prioritization, compliance process improvements, event analyses, reliability assessment, and critical infrastructure protection efforts. This analysis of BES performance provides an industry reference for historical BES reliability, but it also offers analytical insights that lead toward the prioritization of specific actionable risk control steps for industry. These analyses and results are summarized in the annual SOR report, which provides guidance and recommendations for enhanced BPS reliability. Performance Analysis has added Generator Availability Data System (GADS) wind data to the data collected under NERC ROP Section 1600, requiring the development of a new software tool to enable this. In 2019, DA will begin development of the system for solar data collection.

Performance Analysis is working with Event Analysis to develop a link between their databases. Specific equipment outages will be linked to disturbance reports filed with NERC, enabling better association of transmission and generation outages. The continued alignment between these efforts will enhance the ability to conduct effective event analyses as well as to identify key reliability areas for trend analyses of multiple databases. This is expected to improve the depth of event analyses across the ERO Enterprise and expand the quality of data gathered. With use of sophisticated statistical and probabilistic analyses, trends and insights about reliability performance will be identified, as well as effective measures and actions to address reliability risks. Performance Analysis has begun data mining of completed Event Analysis efforts to identify any insights from these events. This is important for as the grid evolves, these events may have been particularly relevant to enhanced grid reliability at the time of the original event investigation.

Performance Analysis is currently refining the composition of NERC's annual SOR report to expand the GADS data trend analysis and, for 2018, has begun reflecting post-seasonal reliability review, insights from analysis of the GADS, Transmission Availability Data System (TADS), and Demand Response Data System (DADS), and integration of event analysis and misoperations. Also, in 2019, the department will implement the decision of whether the SOR report should move from a Q1–Q4 report to a Q4–Q3 report. Current dynamics around validation and reporting of corporate metrics might even move the SOR report to a Q3–Q2 reporting to accommodate the needs of this activity within a common reporting framework.

Further, Performance Analysis continues to work closely with other organizations, including but not limited to EPRI, DOE, IEEE, INPO, NATF, NAGF, and CEA. Performance Analysis collaborates with these groups on a number of fronts, including the TADS, GADS, and DADS.

2019 Goals and Deliverables

In 2019, Performance Analysis has a number of specific goals and deliverables in support of the *ERO Enterprise Operating Plan,* including:

- Issue the SOR report, guidelines, recommendations, and Alerts as needed (including the verification and validation of data and information through Regional Entities and technical committees, as required).
- Provide support and leadership to the OC, Operating Reliability Subcommittee (ORS), and RS and its working groups, the FWG, IIWG, and RWG, with emphasis on balancing operations and analysis, administration of balancing standards, and performance-based outreach to functional entities responsible for real-time BPS reliability.
- Continue the administration of the BAL standards, with emphasis on BAL-003-1 Frequency Response.
- Provide technical assistance to Compliance Assurance and Enforcement with emphasis on BAL-003-1 for the BA performance requirements that became effective in 2017.
- Develop quarterly BPS performance reports using PI Historian data and functionality to support the OC and RS.
- Oversee and evaluate reliability trends that identify reliability risks by analyzing data contained in GADS, TADS, and DADS, along with reliability metrics and protection and controls system misoperations data.
- Support Reliability Standards development by providing subject matter expertise.
- Provide support and leadership to the PC's subcommittees, working groups, and task forces, with primary focus on the Performance Analysis Subcommittee (PAS) and its subgroups.

- Assist in the development of approaches to registration and provide input to NERC staff in support of the development of CMEP risk elements.
- Conduct major event investigations, analyses, and reporting of major findings, recommendations, and lessons learned that will improve reliability.
- Provide insight on emerging system protection issues, and hand-off any issues gleaned with future implications to RASA.

Additionally, a major effort in 2019 will be the development of the technical report to be filed with FERC, in accordance with the directives set forth in Order 794, in addition to development of the *Frequency Response Annual Analysis Report*. Another major effort in 2019 will be the expansion of the PI Historian to include high speed frequency data from the University of Tennessee at Knoxville, as well as interconnection inertia data to support efforts of the RS and ERSWG.

Resource Requirements

Personnel
No change in FTEs for 2019 from the 2018 budget.

Consultants and Contracts
Performance Analysis's budgeted consultant and contract expenses increased from $572k in 2018 to $654k in 2019, primarily due to an increased need for GADS, TADS, and DADS support. A detailed breakdown of 2018 and 2019 budgeted expenses is shown in *Exhibit B – Consultant and Contract Costs*.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
PERFORMANCE ANALYSIS

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 4,533,448	$ 4,533,448	$ -	$ 4,745,085	$ 211,636
Assessment Stabilization Reserve - Penalties	43,478	43,478	-	-	(43,478)
Total NERC Funding	**$ 4,576,927**	**$ 4,576,927**	**$ -**	**$ 4,745,085**	**$ 168,158**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	50,000	50,000	-	40,000	(10,000)
Workshops	-	-	-	-	-
Interest	6,495	4,872	(1,624)	12,162	5,666
Miscellaneous	-	-	-	-	-
Total Funding	**$ 4,633,422**	**$ 4,631,798**	**$ (1,624)**	**$ 4,797,247**	**$ 163,825**
Expenses					
Personnel Expenses					
Salaries	$ 1,372,376	$ 1,406,288	$ 33,912	$ 1,427,724	$ 55,348
Payroll Taxes	92,361	92,683	322	94,388	2,027
Benefits	154,799	156,300	1,500	164,521	9,721
Retirement Costs	154,224	172,952	18,728	160,318	6,094
Total Personnel Expenses	**$ 1,773,760**	**$ 1,828,222**	**$ 54,462**	**$ 1,846,951**	**$ 73,191**
Meeting Expenses					
Meetings	$ 11,000	$ 11,000	$ -	$ 11,000	$ -
Travel	80,000	78,640	(1,360)	80,000	-
Conference Calls	-	1,490	1,490	3,600	3,600
Total Meeting Expenses	**$ 91,000**	**$ 91,130**	**$ 130**	**$ 94,600**	**$ 3,600**
Operating Expenses					
Consultants & Contracts	$ 572,030	$ 572,030	$ -	$ 653,565	$ 81,535
Office Rent	-	-	-	-	-
Office Costs	57,812	47,636	(10,176)	76,290	18,478
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	143,999	143,999	-	295,995	151,996
Total Operating Expenses	**$ 774,341**	**$ 764,165**	**$ (10,176)**	**$ 1,026,350**	**$ 252,009**
Total Direct Expenses	**$ 2,639,101**	**$ 2,683,518**	**$ 44,416**	**$ 2,967,901**	**$ 328,799**
Indirect Expenses	**$ 2,103,037**	**$ 2,328,052**	**$ 225,015**	**$ 2,208,989**	**$ 105,952**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 4,742,138**	**$ 5,011,569**	**$ 269,431**	**$ 5,176,890**	**$ 434,751**
Change in Assets	**$ (108,716)**	**$ (379,771)**	**$ (271,055)**	**$ (379,643)**	**$ (270,927)**
Fixed Assets					
Depreciation	$ (143,999)	$ (143,999)	$ -	$ (295,995)	$ (151,996)
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	35,283	38,105	2,822	(83,648)	(118,931)
Inc(Dec) in Fixed Assets (B)	**$ (108,716)**	**$ (105,894)**	**$ 2,822**	**$ (379,643)**	**$ (270,927)**
TOTAL BUDGET (=A+B)	**$ 4,633,422**	**$ 4,905,675**	**$ 272,253**	**$ 4,797,247**	**$ 163,825**
FTEs	**9.40**	**9.53**	**0.13**	**9.40**	**-**

Electricity Information Sharing and Analysis Center

E-ISAC (including CRISP) (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	29.14	37.60	8.46
Direct Expenses	$ 15,056,942	$ 18,164,321	$ 3,107,379
Indirect Expenses	6,519,415	8,891,220	2,371,805
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	274,241	245,023	(29,217)
TOTAL BUDGET	$ 21,850,597	$ 27,300,563	$ 5,449,966

Background and Scope

The E-ISAC reduces cyber and physical risk to the electricity industry across North America by providing unique insights, leadership, and coordination. NERC formed the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) in 1998 when the U.S. Secretary of Energy requested that NERC serve as the ISAC[32] for the Electricity Subsector.[33] NERC rebranded the ES-ISAC to the Electricity Information Sharing and Analysis Center (E-ISAC) in September 2015. The current E-ISAC organizational structure is designed to support the three primary focus areas in support of its long-term strategy, which is discussed further below: information sharing, analysis, and engagement. The Programs and Engagement group manages the portfolio of E-ISAC products and services and is focused on ensuring stakeholder needs are understood and addressed. The Operations group consists of four teams; of them, the Watch Operations team and CRISP team are primarily focused on information sharing, while the Cyber and Physical teams are focused on deeper analysis of incidents, threats, and mitigations. Both of the main groups support each other across the three focus areas wherever possible.

The E-ISAC also oversees CRISP, a unique public-private initiative between the E-ISAC, the North American electric utility industry, the DOE, and the U.S. Intelligence Community that delivers real-time, relevant, and actionable cybersecurity risk information to all E-ISAC member electricity asset owners and operators. The program leverages subject matter expertise and resources from the E-ISAC, DOE, the Pacific Northwest National Laboratory (PNNL), and the Argonne National Laboratory. Using passive information sharing devices (ISD) on participant networks outside boundary firewalls, packet header information is collected. The CRISP participation agreement contains strict data-handling procedures and guidelines. Participant data is used and then matched against known threat signatures—classified and unclassified—to identify potential threats and provide participants with recommended mitigation steps. Aggregated indicators of compromise and other relevant security information are shared with all E-ISAC members, regardless of participation in CRISP.

Additionally, since 2011, the E-ISAC has sponsored a biennial grid security exercise (GridEx). This geographically-distributed exercise is designed to exercise the electricity industry's crisis response in handling simulated coordinated cyber and physical security threats and incidents, to strengthen utilities' crisis response functions and relationships with government emergency managers and law enforcement, and to provide input for lessons learned. Most recently, GridEx IV, held in November 2017, consisted of a

[32] In 1998, US Government authorities that were derived from Presidential Decision Directive 63, established the Information Security Analysis Center (ISAC) construct. The E-ISAC focuses specifically on information sharing, analytics and sector activities directly related to the protection of critical infrastructure.

[33] Subsequent administrations have sought to continue and strengthen information sharing in other sectors by establishing other sector-specific ISACs. In 2013, the DOE again reaffirmed its desire for NERC to continue to operate the E-ISAC.

two-day grid-focused operational exercise for participants across North America and a half-day tabletop discussion for executives. Over 6,500 participants from 450 industry and government organizations participated in GridEx IV. The E-ISAC manages the program and collects industry information during and after the exercise, subject to existing data collection and protection policies. During the exercise, E-ISAC watch and analysis staff exercise the E-ISAC mission and share crisis information and analysis towards mitigating the threats and attacks. Lessons learned and recommendations are shared with exercise participants via restricted reports, and are also shared publically at a high level.

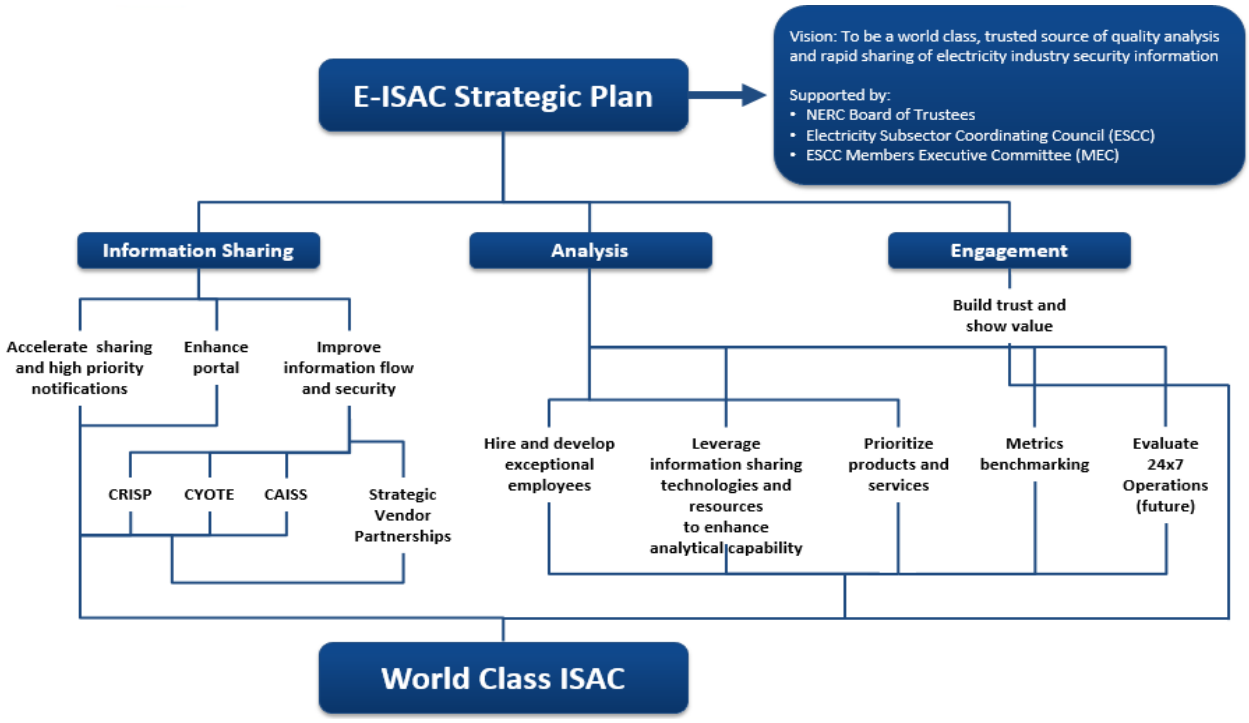
Also since 2011, NERC has also sponsored an annual grid security conference (GridSecCon). This conference brings together hundreds of industry and government subject matter experts on cyber, physical, and operations technology threats and solutions, with training sessions and classified or official use briefs on topics vital to grid security. The E-ISAC provides expertise and gathers appropriate speakers, panelists, and training providers.

E-ISAC staff also routinely engages stakeholders through monthly briefings and threat workshops. The briefings cover timely physical and cyber security topics with regards to critical infrastructure protection. Private and government partner representatives, including those from the U.S. Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC), regularly discuss current events and risk mitigation strategies within the electricity industry audience. Special guest speakers from industry or security analysis firms also provide coverage of emerging threats and mitigation information.

Key Efforts Underway: E-ISAC Long-Term Strategy

At the request of the Board and under the guidance of the ESCC and the ESCC MEC, E-ISAC executive leadership developed a long-term strategic plan, a copy of which is included as *Exhibit E – E-ISAC Long-Term Strategy*. The goal of the long-term strategic plan is to build the E-ISAC into a world-class, trusted source of quality analysis and rapid sharing of electricity industry security information. The MEC approved the long-term strategy on April 24, 2017. The strategy was accepted by the Board on May 11, 2017 and incorporated into NERC's 2018 BP&B that was approved by both the Board and FERC. The E-ISAC's long-term strategy contemplates a measured increase in resources over a five-year period, with the exact timing of resource additions dependent on progress in execution of the long-term strategy and NERC's annual BP&B process. Resource increases to augment existing capabilities for 2019 are detailed below under *2019 Goals and Deliverables*, and in the attachment to Exhibit E, *Expanding E-ISAC Operations to Include 24x7 Onsite Operations.*

The three primary elements of the E-ISAC's long-term strategy are depicted in the chart below: information sharing, analysis, and engagement.



Information Sharing

Timely and effective information sharing is critical to security risk identification and mitigation. Long-term strategy focus areas include the development and implementation of high priority notification procedures, automated information sharing technology, improving the functionality of the E-ISAC portal, and improving access of personnel to classified intelligence sources. The E-ISAC communication portal capabilities include publishing immediate notifications and other informational products, exchanging threat indicator information, and providing self-service access to user security awareness services. With the support of the IT department, the E-ISAC installed a completely new communication portal, incorporating important enhancements with improved functionality and capabilities, such as facilitating direct data exchange with E-ISAC members, other ISACs, and government partners, and establishing user communities that allow registered users to discuss security issues.

Additionally, beyond the portal notifications, the E-ISAC developed the Critical Broadcast Program (CBP) to deliver information rapidly to stakeholders about emerging security threats, based on the best analysis available at the time, with follow-on updates as more details emerge. The CBP allows a faster response to events and a higher level of awareness for members provided by E-ISAC analysts.

The E-ISAC has also broadened automated information sharing capabilities beyond CRISP, piloting a program using the Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information (STIX/TAXII) protocols in use by many organizations, including the DHS. During 2017 and early 2018, the E-ISAC and several industry partners piloted the Cyber Automated Information Sharing System (CAISS). The pilot evaluated technological solutions for bi-directional communication, workflow between participants, the handling and vetting of shared information, and lessons learned from the technology and processes overall. The CAISS pilot will transition to an operational program in 2018 and will be available for voluntary participation from industry asset owners and operators.

Analysis

E-ISAC management is making strategic investments in hiring and training skilled security analysts, identifying and leveraging additional technology, enhancing relationships with and access to government analysis sources, and developing strategic vendor relationships. Working with the NERC IT department, the E-ISAC is building a high-capacity data warehouse to support increasingly complex analytical needs. The data warehouse will assimilate all of the data feeds (including CRISP data) and allow greater correlation and pattern analysis by E-ISAC staff.

Building and maintaining highly skilled cyber and physical security analysis teams is a focus for the E-ISAC, and resource additions are necessary to provide the advanced skills required for analysis in an evolving and complex threat environment. The E-ISAC will also evaluate and where appropriate contract with outside service providers with security analysis expertise to support highly specialized analytical needs, as well as to supplement in-house capabilities.

The E-ISAC is also evaluating several strategic vendor relationships to provide additional data sources from an even wider range of industry participants to both strengthen and enhance existing programs, such as CRISP and CAISS. Available data sources, together with associated technological and analytical capabilities, will be identified, evaluated and, as appropriate, piloted with E-ISAC members to ensure viability.

Engagement

Successful engagement with the electric sector and other stakeholders is critical to cyber and physical security risk identification and mitigation. There are many factors affecting increasing industry engagement, but perhaps the most vital is the trust of the members that shared information is protected. The E-ISAC has made and continues to make significant investments in physical and cyber security systems, procedures, training, and testing to ensure the security of industry data, and adopted a code of conduct to programmatically safeguard information shared by members.

After a successful pilot phase with several Large Public Power Council members, the E-ISAC recently launched an industry augmentation program that embeds industry security analysts at the E-ISAC to interact with E-ISAC staff, observe data collection and handling procedures, and share their own expertise with E-ISAC personnel. Participants also provide valuable feedback regarding their organizations security practices and needs, which helps inform ongoing and future practices and programs within the E-ISAC.

The E-ISAC also regularly interacts with industry members, in coordination with the National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), EEI, and CEA, by providing analyst briefings and information regarding E-ISAC programs and services. Through regional security events, such as NRECA's Rural Cooperative Cybersecurity Capabilities Program, the E-ISAC ensures that actionable security information is available across the industry landscape. The location of GridSecCon is rotated through a different Regional Entity each year. The E-ISAC is committed to being responsive to the needs of the wide range of industry members.

As described above, the new E-ISAC portal includes a user community capability that will allow groups of stakeholders with similar security concerns to collaborate directly with E-ISAC staff on a trusted, secure platform. Building on lessons learned from CRISP participants, the user communities will bring together expertise regarding common areas of issue and build trust through increased interaction among stakeholders.

Additionally, the E-ISAC is continually working to strengthen relationships between industry and government. These relationships are practiced regularly during GridEx and other exercises, and help build understanding between stakeholders that would be vital in responding to any crisis to the grid. Interfacing

smoothly with the government intelligence community would bring with it increased access to government-informed threat information and analysis, and a proposed specific function of additional E-ISAC staff. The E-ISAC is also engaged in regular communications with the DOE, DHS, and the FERC Office of Energy and Infrastructure Security, as well as continuing to build on its cross sector relationships with the other ISACs (financial sector, water, communications, and nuclear).

2019 Goals and Deliverables

The E-ISAC remains focused on furtherance of the strategic efforts discussed above as 2019 marks the second year of the *E-ISAC Long-Term Strategy*. The following discusses areas of increased resource needs to fulfill strategic efforts in 2019 and the overall impact to the E-ISAC budget.

Resources for 2019 Strategy

Watch Operations is the principal entry and egress point for information sharing between the E-ISAC and its members and partners. Information—both required reporting as well as voluntary shares—flows into the organization via portal postings, emails, phone calls, and other means and receives initial analysis by Watch Officers to determine (1) the severity of the event, (2) if it is part of an ongoing series of related event, and (3) whether it rises to the level that requires a "deeper dive" by cyber and physical security subject matter experts. The results of that analysis are shared in a format of greatest benefit to the recipient (operational intelligence for network defenders, recommended actions for leadership, the CBP, etc.). In effect, Watch Operations is responsible for sharing the "so what" that best allows the stakeholders to take the appropriate actions.

With the full support and encouragement of the MEC, the E-ISAC has evaluated resource requirements and options to phase in a 24x7 capability to more rapidly respond to threats outside of normal business hours, beyond a Watch Officer duty rotation. Details of this evaluation are available in the attachment to Exhibit E, *Expanding E-ISAC Operations to Include 24x7 Onsite Operations.*

The E-ISAC also requires expertise necessary to maintain critical links with the intelligence community, which is vital to supporting core analytical and information sharing functions. Key responsibilities of the Government Intelligence Interface team include (1) gathering intelligence community information relevant to the electricity sector and making timely reports of this information (edited as appropriate to avoid disclosure of classified information) available to industry through the E-ISAC, (2) providing electricity sector subject matter expertise required by the intelligence community to inform their intelligence efforts and enhance electricity sector security, (3) facilitating recurring threat update briefings with industry leadership and technical management at both secret and higher classification levels, and (4) supporting collaborative analysis of information between the E-ISAC and the intelligence community.

In support of the needs discussed above, in 2019 resources are being added to the E-ISAC as follows: four cyber analysts, four Watch officers (two for 24x7 capabilities), and one addition to the Government Intelligence Interface team. This increase is primarily to address immediate needs for increased analytical capabilities and expanded watch capabilities outside standard working hours as a first phase in providing the necessary resources for 24x7 operations. In addition, to support E-ISAC operations, two corporate support positions are being added, one in IT (business requirements analyst) and one in the finance area (budget analyst), as further outlined in the long-term strategy.

Additionally, the nature of evolving security threats requires ongoing specialized training and education for E-ISAC staff. As mentioned in the analysis section above, each technically-focused staff member requires significant resources to stay current in their field of expertise and obtain or maintain their certifications. Training requirements for 2019 have been identified and are reflected in personnel expense.

Budget Impacts of 2019 Strategy

The total budget increase for E-ISAC in 2019 is $5.5M, of which $3.5M is attributed to the costs for the second year of the E-ISAC long-term strategy. Building on the resources and foundation put in place in the 2018 BP&B, the E-ISAC 2019 budget reflects a continued measured approach in strengthening the required resources and technology required to support the three primary elements of the E-ISAC's long-term strategy: information sharing, analysis, and engagement.

Resource Requirements

Personnel

The increase of 9 positions (8.46 FTEs) is to address the analytical capabilities discussed above in support of the long-term strategy for the E-ISAC. An additional two positions (1.88 FTEs) are being added to Administrative Programs areas.

Consultants and Contracts

Consultant and contract expenses for the E-ISAC for 2019, including CRISP, are approximately $8.3M, which is an increase of $886k from the 2018 budget. CRISP's consultant and contracts expenses are $6.5M, which is $166k more than was in the 2018 budget. Total E-ISAC increases in 2019 are largely due to funding for GridEx planning, funding for vendor support costs to advance CRISP and other cyber security program participation by smaller municipal utilities, further enhancing the E-ISAC portal capabilities, and strengthening overall analytical capacity and capabilities. A detailed breakdown of the budgeted 2018 and 2019 costs is provided in *Exhibit B – Consultant and Contractor Costs*.

Other Costs

The $250k increase for leasehold improvements is for facility costs associated with the growth if the E-ISAC in support of the E-ISAC long-term strategy. The $200k increase for computer and software capital expenditures is attributed to the upgrade for SAFNR, for which the total capital expenditure of $600k is split between Situation Awareness and the E-ISAC.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
E-ISAC (including CRISP)

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 14,297,524	$ 14,297,524	$ -	$ 19,718,333	$ 5,420,808
Assessment Stabilization Reserve - Penalties	134,783	134,783	-	-	(134,783)
Total NERC Funding	**$ 14,432,307**	**$ 14,432,307**	**$ -**	**$ 19,718,333**	**$ 5,286,026**
Third-Party Funding	$ 7,324,253	$ 7,225,735	$ (98,518)	$ 7,456,449	$ 132,196
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	70,000	70,000	-	70,000	-
Interest	24,038	45,111	21,074	55,782	31,744
Miscellaneous	-	-	-	-	-
Total Funding	**$ 21,850,597**	**$ 21,773,153**	**$ (77,444)**	**$ 27,300,563**	**$ 5,449,966**
Expenses					
Personnel Expenses					
Salaries	$ 4,634,838	$ 4,526,371	$ (108,467)	$ 6,301,432	$ 1,666,594
Payroll Taxes	290,702	270,704	(19,998)	392,466	101,764
Benefits	578,849	576,721	(2,128)	830,430	251,581
Retirement Costs	499,793	500,761	968	672,002	172,209
Total Personnel Expenses	**$ 6,004,182**	**$ 5,874,557**	**$ (129,625)**	**$ 8,196,329**	**$ 2,192,147**
Meeting Expenses					
Meetings	$ 127,000	$ 127,000	$ -	$ 127,000	$ -
Travel	291,000	324,736	33,736	291,000	-
Conference Calls	-	4,794	4,794	-	-
Total Meeting Expenses	**$ 418,000**	**$ 456,530**	**$ 38,530**	**$ 418,000**	**$ -**
Operating Expenses					
Consultants & Contracts	$ 7,391,794	$ 7,391,794	$ -	$ 8,278,000	$ 886,206
Office Rent	-	-	-	-	-
Office Costs	907,330	736,154	(171,176)	903,196	(4,134)
Professional Services	250,000	225,758	(24,242)	250,000	(0)
Miscellaneous	500	500	-	500	-
Depreciation	85,136	85,136	-	118,296	33,160
Total Operating Expenses	**$ 8,634,760**	**$ 8,439,343**	**$ (195,418)**	**$ 9,549,992**	**$ 915,232**
Total Direct Expenses	**$ 15,056,942**	**$ 14,770,430**	**$ (286,512)**	**$ 18,164,321**	**$ 3,107,379**
Indirect Expenses	**$ 6,519,415**	**$ 5,933,723**	**$ (585,692)**	**$ 8,891,220**	**$ 2,371,805**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 21,576,357**	**$ 20,704,153**	**$ (872,204)**	**$ 27,055,540**	**$ 5,479,184**
Change in Assets	**$ 274,241**	**$ 1,069,001**	**$ 794,760**	**$ 245,023**	**$ (29,217)**
Fixed Assets					
Depreciation	$ (85,136)	$ (85,136)	$ -	$ (118,296)	$ (33,160)
Computer & Software CapEx	100,000	100,000	-	300,000	200,000
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	150,000	150,000	-	400,000	250,000
Allocation of Fixed Assets	109,377	97,121	(12,256)	(336,681)	(446,057)
Inc(Dec) in Fixed Assets (B)	**$ 274,241**	**$ 261,985**	**$ (12,256)**	**$ 245,023**	**$ (29,217)**
TOTAL BUDGET (=A+B)	**$ 21,850,597**	**$ 20,966,138**	**$ (884,460)**	**$ 27,300,563**	**$ 5,449,966**
FTEs	**29.14**	**24.29**	**(4.85)**	**37.60**	**8.46**

Training, Education, and Personnel Certification

Training, Education, and Personnel Certification (in whole dollars)	2018 Budget	2019 Budget	Increase (Decrease)
Total FTEs	5.88	4.94	(0.94)
Direct Expenses	$ 1,708,013	$ 1,579,638	$ (128,375)
Indirect Expenses	1,314,398	1,159,719	(154,679)
Other Non-Operating Expenses	-	-	-
Inc(Dec) in Fixed Assets	20,613	(45,834)	(66,447)
TOTAL BUDGET	$ 3,043,024	$ 2,693,523	$ (349,501)

Background and Scope

Training and Education

The Training and Education program provides oversight for coordination and delivery of learning materials, resources, and activities to allow for training and education of (1) ERO Enterprise staff supporting statutory and delegation-related activities and (2) BPS industry participants consistent with ERO functional program requirements.

The Training and Education program supports NERC's responsibilities to develop, adopt, and obtain approval of Reliability Standards and to monitor, enforce, and achieve compliance with the mandatory standards. Section 901 of the NERC ROP addresses the program's obligations to industry stakeholders and ERO Enterprise staff. The responsibility to participate in the program is shared among the NERC departments,[34] in conjunction with the ERO Enterprise working groups.

NERC's Continuing Education program acknowledges high-quality learning activities within the electric utility industry by approving continuing education providers that meet NERC guidelines and standards. System Operator Certification, which is detailed below, is maintained by completing NERC-approved continuing education courses and activities. The OC's Personnel Subcommittee, composed of industry training experts, provides oversight of the Continuing Education program. Section 902 of the NERC ROP addresses the specific continuing education program expectations and activities.

Personnel Certification

The System Operator Certification program ensures that personnel operating the BPS have the skills, training, and qualifications needed to operate the system reliably. NERC maintains credentials for over 7,500 System Operator credential holders who work in various industry areas across North America. NERC's System Operator Certification exam is designed to test specific knowledge of job skills and Reliability Standards, and prepares operators for complying with requirements of Reliability Standards and appropriately operating the BPS during normal and emergency operations. The System Operator Certification program is governed by the NERC Personnel Certification Governance Committee (PCGC), an industry group of operations experts, trainers, and supervisors. Certification exams are created by the PCGC's Exam Working Group (EWG), an industry group of operations subject matter experts. Under the PCGC oversight, the EWG reviews and updates job tasks and certification exams. Section 600 of the NERC ROP addresses the Personnel Certification activities in the area of System Operator Certification.

[34] The Human Resources department is also engaged in training initiatives.

Key Efforts Underway

Training and Education
The ERO provides learning materials, resources, and activities to assist industry and ERO Enterprise staff in their understanding of key program areas. These areas include:

- Reliability Standards;
- Risk-based compliance monitoring and enforcement;
- Organization Registration and Certification;
- Event Analysis, cause analysis, Performance Analysis, and lessons learned;
- RASA; and
- Continuing education for System Operators.

Personnel Certification
The Personnel Certification department is performing the following activities:

- Continuing to update the System Operator Certification Exam Item Bank to ensure relevance to current Reliability Standards and promote reliability of the BPS;
- Developing the exam "skills assessment" process to better assess the skills and knowledge of System Operators;
- Developing a strategic plan for the System Operator Certification program; and
- Evaluating credential review and rationalization to maintain credentials.

Additionally, the PCGC approved and launched the System Operator Certification Continuing Education Database (SOCCED) to a new platform in 2018. The new platform will provide accurate and meaningful data to assist with the System Operator Certification program.

2019 Goals and Deliverables

Training and Education
The annual NERC and ERO Enterprise Learning Priorities Plan articulates and prioritizes the accumulated learning needs for the ERO Enterprise and the potential delivery vehicles supporting achievement of the *ERO Enterprise Operating Plan* goals. Development and management of the annual plan is exercised through monthly meetings to ensure priorities are reviewed and updated based on the changing business landscape informed through input received by the various functional program managers on behalf of their respective programs, ERO Enterprise working groups, and leadership teams.

An objective-based approach describing audience needs facilitates identification and formulation of products throughout the year. It inspires modular (interchangeable parts or building blocks) thought in implementing a cross-cutting multi-use product model. Production is accomplished by combining in-house expertise and tools with vendor support to increase bandwidth that positively impacts the quality and timeliness of customer service.

NERC program leads spearhead the effort to identify gaps in program knowledge and associated learning needs of their employees, industry stakeholders, and ERO Enterprise partners. The following objectives serve as foundational building blocks for ongoing learning development work and will inform the priorities of focus in 2019 and beyond:

- Educate industry on managing risk to the reliability of the BPS based on the results of technical assessment and analysis, standards development, and human performance knowledge.
- Enhance ERO Enterprise compliance monitoring personnel performance through a deeper understanding of ERO Enterprise compliance monitoring processes and technical aspects of the BPS operations.
- Improve NERC employee understanding of NERC functions and core technical knowledge for regulating the BES.

NERC will deliver training and education products and resources by hosting workshops and webinars, as well as computer-based and instructor-led training courses. The responsibility for subject matter expertise input to the learning development process is shared among multiple departments at NERC. The Training and Education department provides coordination and synchronization efforts for shared NERC and ERO Enterprise learning responsibilities in addition to advancing and improving the skills of the NERC operating staff. The Human Resources department funds and manages the delivery of individual corporate employee training and continuing education programs in concert with the coordination efforts of the Training and Education department.

The Continuing Education program evaluates and revises the current program criteria as reflected in the program manual. The evaluation considers the growth and maturation of industry programs, as well as ongoing research in the area of adult learning to ensure that the Continuing Education program efforts improve core objectives in addition to fostering improvement of training and promoting quality industry training programs in general. The Continuing Education program will remain focused on NERC System Operator credential maintenance in 2019. The program will share funding responsibilities with the Personnel Certification program for SOCCED and the associated help desk tool.

Personnel Certification

With the successful delivery of the certification exams using Linear on the Fly Testing (LOFT), which is the dynamic creation of exams, the PCGC has reduced the exam delivery cycle from 36 months to a dynamic process every time an exam is initiated by a candidate. As part of the ongoing exam development cycle, the EWG will continue to develop and analyze new items for future certification exams and ensure relevancy to current Reliability Standards.

In 2019, the PCGC will focus on further development of the System Operator Certification program strategic plan, which will include but is not limited to analyzing data from the System Operator Certification program survey and white papers to the industry. The PCGC is dedicated to enhancing the System Operator Certification program to assure reliable operation of the BPS. Key deliverables for the System Operator Certification program include:

- Annual analysis of the System Operator Certification Exam Item Bank;
- New exam items;
- Enhancement to the credential maintenance tool; and
- Strategic plan action items for program enhancements.

Personnel Certification will continue to work with industry stakeholders and the exam development vendor to create certification exams that will promote reliability of the BPS.

Resource Requirements

Personnel

The reduction in FTEs is the result of the elimination of one open position (0.94 FTEs) from the Training, Education, and Personnel department.

Consultants and Contracts

Consultant and contract expenses increased to $385k for 2019 from $348k in 2018, primarily for System Operator Certification solution support. A detailed breakdown of 2018 and 2019 budgeted expenses is shown in *Exhibit B – Consultant and Contract Costs*.

Other Costs

The $64k increase for office costs is due primarily to software subscription and support costs for the new database system, which is being reclassified from contracts & consultants in the 2018 budget.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
TRAINING, EDUCATION, and PERSONNEL CERTIFICATION

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ 1,309,031	$ 1,309,031	$ -	$ 1,031,115	$ (277,916)
Assessment Stabilization Reserve - Penalties	17,391	17,391	-	-	(17,391)
Total NERC Funding	**$ 1,326,422**	**$ 1,326,422**	**$ -**	**$ 1,031,115**	**$ (295,307)**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	1,790,000	1,728,075	(61,926)	1,790,000	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	4,060	4,444	385	6,385	2,325
Miscellaneous	-	-	-	-	-
Total Funding	**$ 3,120,482**	**$ 3,058,941**	**$ (61,541)**	**$ 2,827,500**	**$ (292,982)**
Expenses					
Personnel Expenses					
Salaries	$ 701,307	$ 713,474	$ 12,167	$ 589,230	$ (112,077)
Payroll Taxes	52,088	51,742	(346)	43,456	(8,633)
Benefits	95,207	89,780	(5,427)	86,499	(8,709)
Retirement Costs	79,353	89,345	9,992	66,561	(12,791)
Total Personnel Expenses	**$ 927,956**	**$ 944,342**	**$ 16,387**	**$ 785,745**	**$ (142,210)**
Meeting Expenses					
Meetings	$ 44,250	$ 44,250	$ -	$ 44,250	$ -
Travel	17,000	16,353	(647)	17,000	-
Conference Calls	-	2,981	2,981	1,200	1,200
Total Meeting Expenses	**$ 61,250**	**$ 63,584**	**$ 2,334**	**$ 62,450**	**$ 1,200**
Operating Expenses					
Consultants & Contracts	$ 598,900	$ 598,900	$ -	$ 547,000	$ (51,900)
Office Rent	-	-	-	-	-
Office Costs	117,969	118,986	1,017	182,024	64,055
Professional Services	-	-	-	-	-
Miscellaneous	500	500	-	500	-
Depreciation	1,439	1,439	-	1,919	480
Total Operating Expenses	**$ 718,808**	**$ 719,824**	**$ 1,017**	**$ 731,443**	**$ 12,636**
Total Direct Expenses	**$ 1,708,013**	**$ 1,727,750**	**$ 19,737**	**$ 1,579,638**	**$ (128,375)**
Indirect Expenses	**$ 1,314,398**	**$ 1,409,534**	**$ 95,136**	**$ 1,159,719**	**$ (154,679)**
Other Non-Operating Expenses	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Total Expenses (A)	**$ 3,022,411**	**$ 3,137,284**	**$ 114,873**	**$ 2,739,358**	**$ (283,053)**
Change in Assets	**$ 98,071**	**$ (78,343)**	**$ (176,414)**	**$ 88,143**	**$ (9,928)**
Fixed Assets					
Depreciation	$ (1,439)	$ (1,439)	$ -	$ (1,919)	$ (480)
Computer & Software CapEx	-	-	-	-	-
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	-	-	-	-	-
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	22,052	23,071	1,019	(43,915)	(65,967)
Inc(Dec) in Fixed Assets (B)	**$ 20,613**	**$ 21,632**	**$ 1,019**	**$ (45,834)**	**$ (66,447)**
TOTAL BUDGET (=A+B)	**$ 3,043,024**	**$ 3,158,916**	**$ 115,892**	**$ 2,693,523**	**$ (349,501)**
FTEs	**5.88**	**5.77**	**(0.11)**	**4.94**	**(0.94)**

Administrative Programs

Administrative Programs (in whole dollars)	Direct Expenses and Fixed Assets			FTEs		
	2018 Budget	2019 Budget	Increase (Decrease)	2018 Budget	2019 Budget	Increase (Decrease)
General & Administrative	$ 10,096,147	$ 10,427,465	$ 331,318	15.98	13.16	(2.82)
Legal and Regulatory	2,914,377	3,882,055	967,678	10.34	13.16	2.82
Information Technology	11,266,626	11,547,302	280,677	22.33	23.27	0.94
Human Resources & Administration	1,704,459	2,589,923	885,464	2.82	9.40	6.58
Finance and Accounting	4,008,326	2,689,542	(1,318,785)	15.98	8.46	(7.52)
Total Administrative Programs	**$ 29,989,934**	**$ 31,136,286**	**$ 1,146,352**	**67.45**	**67.45**	-

Program Scope and Functional Description

NERC's Administrative Programs area includes the budget for all business and administrative functions of the organization, including (1) technical committees and member forums; (2) General &Administrative, which includes Board fees and expenses, the CEO, CRO and support staff, communications, external affairs and governmental relations, and office rent; (3) Legal and Regulatory; (4) Information Technology; (5) Human Resources & Administration; (6) Finance and Accounting; and (7) other general administrative expenses necessary to support program area activities. These functions are necessary to the existence and functioning of the organization and support the performance of NERC's ERO statutory activities. The costs of the Administrative Programs functions are allocated to the statutory programs as indirect expenses. The resource requirements and comparative budget information for each of these functions are described below.

Technical Committees and Members' Forum Program

While NERC management and staff will continue to interact with and support numerous reliability-related forums (e.g., the NATF and NAGF), NERC's 2019 budget does not contain specific funding for any forum activities.

General & Administrative

Background and Scope

The General & Administrative area is responsible for the administration and general management of the organization. Expenses allocated in this area include office rent as well as personnel and related costs of (1) the CEO, the CRO, and their support staff; (3) communications, external affairs, and government relations staff; and (4) Board costs. The 2.82 decrease in FTEs is the result of resource allocations to realign staff with current needs. Consultant and contract expenses for this area are increasing $200k due to consulting work for strategic support for the E-ISAC and effectiveness and efficiency initiative.

The following table details the Board costs included in the total costs of the General and Administrative area.

Board of Trustee Expenses	Budget 2018	Budget 2019	Variance 2018 Budget v 2018 Budget	Variance %
Meeting and Travel Expenses				
Quarterly Board Meetings	$ 185,000	$ 185,000	$ -	0.0%
Trustee Travel	130,000	130,000	-	0.0%
Total	**$ 315,000**	**$ 315,000**	**$ -**	**0.0%**
Professional Services				
Independent Trustee Fees	$ 1,237,500	$ 1,289,375	$ 51,875	4.2%
Trustee Search Fees	100,000	100,000	-	0.0%
Total	**$ 1,337,500**	**$ 1,389,375**	**$ 51,875**	**3.9%**
Total	**$ 1,652,500**	**$ 1,704,375**	**$ 51,875**	**3.1%**

The 2018 annual review of trustee compensation is currently being conducted. The increase in independent trustee fees currently shown above is due to of the addition of a trustee per the Board's decision to search for this new trustee in 2018 instead of 2019. This decision was made to reduce the number of trustee searches that would need to be conducted in 2019 as a result of the coinciding term expirations of two current trustees.

Legal and Regulatory

Background and Scope

The Legal and Regulatory department's workload is derived from the following key NERC program areas: Compliance Analysis, Organization Certification and Registration, RASA, Reliability Risk Management, and Reliability Standards. In addition, the Legal and Regulatory department is also responsible for providing a wide range of legal support to the NERC management team regarding antitrust, corporate, commercial, insurance, contract, employment, real estate, copyright, tax, legislation, and other legal matters. The department also addresses legal and regulatory matters that arise in connection with the delegation agreements with the Regional Entities.

Resource Requirements

Personnel

The increase of three positions (2.82 FTEs) is the result of resource allocations to realign staff with current needs.

Professional Services

Outside law firms and consultants supporting this area are budgeted and tracked as Professional Services. The Professional Services budget for 2019 increased $50k as compared to 2018 primarily due to added support costs for the E-ISAC strategy.

Information Technology

Background and Scope

NERC's IT department plan includes capital and operating expenses required to support, build, configure, and enhance applications that serve registered entities, Regional Entities, and NERC staff. The plan also includes work related to ERO Enterprise data analysis, as well as ongoing NERC and E-ISAC internal operations.

The focus of budget funding for 2019 and 2020 is primarily on applications designed to better support effectiveness and consistency across the ERO Enterprise in the areas of Reliability Standards, Compliance Monitoring, Enforcement, Registration, and the associated assessment of reliability risk. These applications include the CMEP Technology Project and complementary solutions for entity registration and standards data. The entity registration application will consolidate core registration functions currently distributed across three applications into a single registration application. In similar fashion, the three applications used across NERC and the Regional Entities for enforcement processing will be replaced by a single common application that also provides compliance monitoring functionality. Additionally, a standards database solution will be developed to work in concert with the compliance and enforcement application. These investments will provide broad benefits across the ERO Enterprise in terms of the effectiveness and efficiency of operations and meeting reliability goals. Additionally, by providing more tools and systems to registered and Regional Entities, associated economies of scale will result from these investments, increasing value across the ERO Enterprise in the years to come.

The 2019–2021 planning period also includes improvements to NERC's public facing website (NERC.com), funding for GADS solar data (GADS Solar), GADS wind data (GADS Wind), and a rewrite or replacement of the Resource Adequacy application.

The IT budget is broken down into four categories as follows:

- **ERO Enterprise new functionality** – Items listed in this category are those items designed to add, enhance, or improve capabilities for registered entities, Regional Entities, and NERC staff. This includes the Entity Registration application, the CMEP Technology Project, NERC.com, and other applications.
- **ERO Enterprise infrastructure and support** – Items listed in this category are those infrastructure and support items required for applications used by registered entities, Regional Entities, and NERC staff. Items include security and applications used by the ERO Enterprise such as The Events Analysis Management System (TEAMS), the Bulk Electric System Notification and Exception System tool (BESnet), the Standards Balloting System (SBS), the Reliability Coordinator Information System (RCIS), User Management and Records (UMR), and numerous other applications.
- **NERC new functionality** – There is no new functionality targeted for NERC in the 2019–2021 planning period. The budget continues to be heavily focused on improving the registered entity and Regional Entity experience.
- **NERC infrastructure and support** – Items listed in this category are primarily those items required to maintain and run the internal office infrastructure and support NERC staff operations, including business continuity and disaster recovery. Items include server hardware and software licenses, network equipment, data and telecommunication circuits, and data storage, as well as office administrative applications (e.g., Microsoft Office) and user hardware such as laptops and peripherals.

A further discussion of each item is outlined below.

ERO Enterprise New Functionality

As noted above, this category is primarily those applications or systems designed to improve or add capability to registered entities, Regional Entities, and NERC staff. Over the past two years, IT has successfully at deployed a number of new applications and functionalities for the ERO Enterprise that have now moved into support. In 2019 and beyond, IT will continue that trend with a heavy focus on Entity Registration and the CMEP Technology Project.

- **Entity Registration** – The objective of the Entity Registration application is to take the core registration functions currently distributed across three systems—the OATI Compliance Data Management System (webCDMS), Guidance Compliance Information Tracking System (CITS), and Guidance Compliance Reporting and Tracking System (CRATS)—and move those functions to a single, consolidated registration system. Doing so will allow for an expansion of current functionality, more control over the future of the application, and ultimate reduction in costs through the long-term transfer of the remaining functions provided by those three systems into a single, common system.

  This program is being implemented via multiple projects over four years. This first project in 2017 addressed the registration, tracking, and management of CFRs. Subsequent projects will address Joint Registration Organizations (JROs), tracking coordinated oversight of MRREs, consolidating all existing entity registration functions into a single platform, adding validation of business relationships and functional responsibilities, and the capability to integrate reliability and compliance data for risk analysis purposes (supporting the creation of an entity's risk profile).

- **CMEP Technology Project** – IT will work closely with the Regional Entities through 2020 to evaluate and implement strategic investments in tools that replace the current three applications mentioned above with a single, consolidated application. Items under consideration at this time include how Reliability Standards data is stored and maintained, as well as how best to support the various parts of the CMEP process (e.g., analysis of risk, development of implementation plans and audit schedules, actual compliance monitoring, and enforcement processing).

  Funding for any capital investments in these areas will be subject to review and approval as part of the BP&B application in the year when such investments are proposed to be made. Prior to actual start of each project, the project will be reviewed through the enterprise information technology investment planning process to ensure the project's estimated costs and benefits are reasonable and justify investment. For more information on this process, see *Robust Planning for New Capital Projects* section below.

- **Additional tools –** IT will continue to support the business in future years though the provision of software products that meet the analysis, communication, data collection, and analysis needs of the ERO Enterprise. Examples include the collection and analysis of solar generation performance data, further analysis of wind generation performance data, additional data collection and analysis to support and enhance reliability assessments, and further improvement of the effectiveness and efficiency of communications with stakeholders and industry participants.

ERO Enterprise Infrastructure and Support

This category primarily consists of items used by registered entities, Regional Entities, and NERC staff. IT has worked closely with the Regional Entities to design and configure a number of ERO Enterprise applications, with a bias toward using commercial-off-the-shelf (COTS) technology whenever possible. Infrastructure and support for these COTS tools (such as SharePoint and the Dynamics xRM platform), as well as custom built applications developed in the past, require ongoing investment to maintain

continuous operations. For many applications and systems, this includes the cost of maintaining development, quality assurance, and staging and production environments, which are required to ensure the security and operational integrity and stability of the multiple applications supported for the ERO Enterprise, including the necessary redundancy and business continuity hardware, network and licenses to ensure operational availability of these important business assets. These applications and systems are monitored, tested (including penetration and vulnerability testing), and maintained in a manner as to ensure the highest level of integrity, security, and availability to the roughly 4,000 users across North America.

IT continues to place emphasis on ensuring the environment is configured in a manner consistent with enterprise best practices, ensuring the security and integrity of the environment while allowing ERO Enterprise users to obtain the information and resources required to perform various analyses. Ongoing support for new applications, such as The Event Analysis Management System (TEAMS), the Misoperations Information Data Analysis System (MIDAS), the Standards Balloting System (SBS), and the Reliability Assessment Data System (RADS), in addition to numerous older ERO Enterprise products (such as GADS, TADS, and DADS), make up this portion of the IT budget.

NERC New Functionality

There is no new functionality planned for the NERC environment in the 2019–2021 planning period.

NERC Infrastructure and Support

As previously noted, NERC infrastructure and support are those items required to maintain and support the internal infrastructure for NERC staff, to include those items necessary for business continuity and disaster recovery. Items such as file servers, network equipment, storage, Microsoft Office (Word, Excel, PowerPoint, Email, SharePoint, etc.), along with security and telecommunications, are required to ensure staff have the necessary tools and technology to perform their daily operational functions. Emphasis continues to be placed on optimizing the amount of effort placed on NERC infrastructure and support in order to minimize spend on internal office steady state operations, allowing a larger portion of IT resources to focus on new ERO Enterprise functionality as well as ERO Enterprise infrastructure and support. Examples of items included in internal operations are outlined below:

- **CRATS** – This compliance database is used to track violations, mitigation plans, and reporting required by NERC as the ERO. The database has additional modules, such as the Reliability Standards, Technical Feasibility Exceptions (TFEs), and Registration module, which contains a list of all registered entities. Funding requirements include ongoing maintenance for the CRATS compliance tool. As noted above, the CRATS application will be replaced in 2020 by an enterprise CMEP tool used by NERC, the Regional Entities, and registered entities. Reduced funding for support of the CRATS application in 2020 and beyond will be required for historical purposes.
- **Meeting manager, ERO membership, central repository of curtailment events** – NERC maintains a number of legacy applications. Many of the legacy applications were developed and implemented five to ten years ago and are unable to benefit from contemporary application development. Some of these applications may have to be completely rewritten, or moved to the xRM application platform, as IT was able to do with Application Broker, NERC MyAccount, and the User Management Program (UMP) in 2016. Funding in 2019–2021 is required for ongoing maintenance and enhancements until the applications can be rewritten or moved to the xRM platform or, in some cases, potentially divested or transferred to industry support.
- **Quarterly penetration and vulnerability testing of all NERC networks and systems** – Expert consulting services to provide intrusion detection and vulnerability testing of NERC.com and NERC's network, applications, and systems, is an essential requirement for operations. NERC is

subject to frequent intrusion attempts where external parties try to gain access to its systems. Any vulnerability identified is documented and provided to NERC IT for rapid remediation.

- **NERC security program** – NERC's IT department performs a number of technology initiatives to ensure the security of the network and infrastructure. In order to continually improve security, a more holistic approach is required that implements technology improvements and constructs an overarching security program to ensure all aspects of security have been considered, including information classification, review of retention policies, and enforcement of security guidelines. Security remains an intensive focus area throughout the 2019–2021 budget cycle and increasing cyber security threats will continue to put pressure on the IT budget to meet demands.

Robust Planning for New Capital Projects

NERC has adopted an enterprise IT investment planning methodology that ensures only projects with compelling and approved business cases are funded. The approval process uses four approval gates:

- Business unit sponsor approval;
- NERC vice president/chief technology officer (CTO) approval;
- ERO Technology Leadership Team (TLT) (comprised of the NERC CEO and three Regional Entity CEOs) approval; and
- Approval from all NERC and Regional Entity CEOs.

NERC's planning process and associated approval gates result in thorough review of both costs and benefits of the proposed technology project prior to moving forward with the project. The benefits of a given project are evaluated within the context of six identified value domains:

- Reducing reliability risk (the project is expected to address one or more identified risks to reliability);
- Increasing capability (the project is expected to make possible activities or analysis that are not currently possible given existing process, resource, or system limitations);
- Reducing corporate risk (the project is expected to address one or more corporate risks, such as reputational risk, contract risk, or litigation risk);
- Increasing work quality (the project is expected reduce the probability of errors or provide information of better quality);
- Increasing productivity (the project is expected to increase the amount of work that can be completed within the same amount of time); and
- Reducing cost (the project is expected to provide a net reduction in costs related to the area(s) being addressed by the project).

As projects progress, complete, and mature, periodic evaluations of the manifesting benefits against the projections used within the business case are performed. This helps to create organizational discipline by ensuring projections are realistic and not unreasonably optimistic. NERC also considers potential benefits to the Regional Entities and registered entities when considering potential IT investments, which ensures recognition of Regional Entity staffing and budget impacts within the business case analysis, identifying economies of scale, and benefits to ERO Enterprise stakeholders through IT investment.

Resource Requirements

Personnel

The FTE increase is the result of the addition of one position (0.94 FTEs) in support of the E-ISAC long-term strategy.

Consultants and Contracts

The consultant and contract budget decreased slightly to $2.0M in 2019 from $2.1M in 2018. A detailed breakdown of 2018 and 2019 budgeted expenses are shown in *Exhibit B – Consultant and Contract Costs*.

IT Office Costs

The below table shows the major categories of IT Office Costs, and a short description of certain categories follows thereafter. Explanations for the major areas of increase from the 2018 budget to the 2019 budget are provided in Table B-8 in Section B.

Office Costs	Budget 2018	Budget 2019	Variance 2018 Budget v 2017 Budget	Variance %
Telephone	$ 162,100	$ 129,911	$ (32,189)	-19.9%
Internet	358,920	303,710	(55,210)	-15.4%
Computer Supplies	98,100	98,100	-	0.0%
Software License and Support*	1,773,030	2,231,000	457,970	25.8%
Subscription and Publications	126,200	131,000	4,800	3.8%
Dues	2,500	2,500	-	0.0%
Express Shipping	7,500	7,500	-	0.0%
Audio/Visual and Hardware Lease**	640,336	752,529	112,193	17.5%
Total	**$ 3,168,686**	**$ 3,656,250**	**$ 487,564**	**15.4%**

**Combined Software and Maintenance/Service Agreement accounts to streamline accounting activities*

***Combined Audio/Visual and Hardware Lease accounts to streamline accounting activities*

Telephone

Telephone costs are items associated with cellular phone, satellite phone (for business continuity), mobile laptop cellular air card, and Session Internet Protocol (SIP) data circuits.

Internet

Internet expense is comprised of both primary and secondary data circuits to ensure continuous capability in the event of primary service provider failure.

Computer Supplies

Computer supplies are expense items required for infrastructure support.

Software License and Support

Includes non-capital software subscription and license costs, and related support agreements. Also includes costs for support and service agreements related to NERC infrastructure management software, data center co-location, offsite backup of data, and network and security monitoring.

Audio/Visual and Hardware Leases

Consists of lease payments for audio visual equipment, computers, laptops, servers, and switches that were leased, in lieu of purchasing, beginning in January 2017.

Fixed Asset (Capital) Expenses

The following table presents a summary of NERC's IT 2019 fixed asset (capital) budget[35] compared to the 2018 budget:

IT Capital Budget	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Hardware (storage, servers)	$ 705,000	$ 465,000	(240,000)	-34.0%
Other Equipment	370,000	425,000	55,000	14.9%
Disaster Recovery	100,000	-	(100,000)	-100.0%
NERC Software Licenses	301,000	120,000	(181,000)	-60.1%
Total	**$ 1,476,000**	**$ 1,010,000**	**$ (466,000)**	**-31.6%**

As in prior years, the goal of the fixed assets (capital) program for the 2019–2021 planning period is to provide access, visibility, and analysis of data from many different sources. This requires ongoing investments in hardware, software, and associated tools. The overarching theme is to securely gather, analyze, and maintain data across the ERO Enterprise to support ERO operations. Adding the capability to centralize and mine data—in addition to foundational elements such as the Microsoft xRM application, SharePoint 2013, and disaster recovery and enhanced security—sets the stage for vastly improved reporting and business intelligence. It also allows the capability for collaboration and sharing of information vital to the ERO's mission.

In addition to the investments described in the preceding paragraph to support efficiency and consistency across the ERO Enterprise, the 2019 budget also includes the cost of network assets, software, servers, laptops, security, and other hardware to support daily operations.

Human Resources & Administration

Background and Scope

Human Resources & Administration primarily includes human resources and facilities and meeting planning functions. NERC's human resources functions include staffing, benefits administration, employee relations, performance and compensation management, and training and development. Management has implemented a robust, objective, and auditable performance management system to track corporate and individual performance against pre-established goals, objectives, and measures. Each year NERC continues to refine and improve this system.

Leadership, Management, and Professional and Administrative Staff Training and Development

As part of the ERO Enterprise's ongoing efforts to engage and retain highly qualified talent with the leadership and technical skills to support its mission, NERC's executives, managers, and professional and support staff participate in ongoing training and development to improve competencies critical to success and succession planning for critical roles. As such, NERC will continue to invest in learning opportunities in several areas. First, Human Resources will continue to host and optimize an e-leaning platform, SkillSoft, to provide staff resources for improving soft and technical skills. Second, Human Resources will provide broad-based staff development training though real-world access via tours of and training on control centers, electric substations, and power generation plants. Finally, staff will have access to additional

[35] NERC's total 2019 fixed asset (capital) budget is $4.8M and includes $3.3M for ERO Application Development. These ERO projects are managed by NERC's IT department but the costs are budgeted in the applicable NERC program area.

education, including but not limited to degree-oriented university education, pursuit of specialized certifications, and other in-house and external training that provides essential competencies and skills development that will lead to improved organization performance.

Compensation Strategy
NERC relies on data and advisory from multiple perspectives to hire and retain the necessary technical and other staff to support the goals and objectives in the company's operating plan. Under the mandate of the Board Corporate Governance and Human Resources Committee (CGHRC), NERC performs periodic market compensation studies to benchmark the pay practices of similar organizations and roles for which NERC hires. To ensure that NERC is able to attract the best-qualified staff to meet our mission, the CGHRC recommended a compensation philosophy of paying between the 50th and 75th percentiles, which has historically enabled the company to hire appropriate skills at prevailing market rates. Management will continue to closely monitor market conditions through periodic compensation studies and real-time pay trends of our candidate pool and expect that our pay philosophy will sustain the ability to hire qualified talent consistent with appropriate market levels.

Compensation Consulting
Consultants are periodically retained to examine appropriate compensation based on current market data. This ensures that decisions affecting compensation are made in light of the current market climate and that qualified employees are attracted and retained within a defined total remuneration range. NERC also periodically retains compensation subject matter experts to perform periodic assessments of the Board compensation model to ensure alignment with market practices.

Surveys
NERC periodically retains a vendor to conduct Board and committee effectiveness surveys to identify improvement opportunities. Human Resources will also launch additional surveys as appropriate, based on business needs, which may include periodic internal climate surveys.

Succession Planning
Minimizing disruption of knowledge, skill, and experience of key staff is critical to the company's success. Human Resource works with senior management to identify essential roles and develop strategies to build succession and contingency plans for any loss of staff.

Human Resources Products and Services Automation
Human Resource will continue to operate, maintain, and investigate investment in additional electronic platforms for Human Resource support services that reduce administrative burden and improve employee access to tools and information.

Resource Requirements

Personnel
The increase of seven positions (6.58 FTEs) is the result of a reclassification from the finance and accounting department to human resources and administration to better reflect actual activities and functions.

Consultants and Contracts
The consultant and contract budget increased to $690k in 2019 from $640k in 2018 primarily due to increased funding for human resources and compensation-related consulting services. A detailed breakdown of 2018 and 2019 budgeted expenses is shown in in *Exhibit B – Consultant and Contract Costs*.

Miscellaneous Expenses

Miscellaneous expenses include community responsibility and employee engagement, the year-end employee appreciation event, and employee rewards and recognition.

Finance and Accounting

Background and Scope

NERC's Finance and Accounting department manages all finance and accounting functions, including employee payroll, 401(k), 457(b), and 457(f) plans, travel and expense reporting, monthly financial reporting, sales and use tax, meeting and events planning and services, insurance, internal auditing, and facilities management. This area also holds primary responsibility for the development of the annual BP&B, as well as NERC's ERO risk management framework. Over the past several years, NERC's Finance and Accounting department implemented additional policies, procedures, and controls governing day-to-day practices including contract and personnel procurements, meetings, conference planning and travel, expense reimbursement, and back office systems and procedures. The department will continue to refine, improve and, where necessary, implement additional procedures and controls.

Resource Requirements

Personnel

The reduction of eight positions (7.52 FTEs) is primarily the result of a reclassification from the finance and accounting department to the human resources and administration department to better reflect actual activities and functions.

Consultants and Contracts

The consultant and contract budget increased to $475k in 2019 from $427k in 2018 primarily for outside auditor consulting support for various risk management and internal control and audit intiatives. A detailed breakdown of 2018 and 2019 budgeted expenses is shown in *Exhibit B – Consultant and Contact Costs*.

Statement of Activities and Fixed Assets Expenditures
2018 Budget & Projection, and 2019 Budget
ADMINISTRATIVE SERVICES

	2018 Budget	2018 Projection	Variance 2018 Projection v 2018 Budget Over(Under)	2019 Budget	Variance 2019 Budget v 2018 Budget Over(Under)
Funding					
ERO Funding					
NERC Assessments	$ (231,393)	$ (231,393)	$ -	$ (1,067,980)	$ (836,587)
Assessment Stabilization Reserve - Penalties	-	-	-	-	-
Total NERC Funding	**$ (231,393)**	**$ (231,393)**	**$ -**	**$ (1,067,980)**	**$ (836,587)**
Third-Party Funding	$ -	$ -	$ -	$ -	$ -
Testing Fees	-	-	-	-	-
Services & Software	-	-	-	-	-
Workshops	-	-	-	-	-
Interest	-	192,706	192,706	-	-
Miscellaneous	-	-	-	-	-
Total Funding	**$ (231,393)**	**$ (38,687)**	**$ 192,706**	**$ (1,067,980)**	**$ (836,587)**
Expenses					
Personnel Expenses					
Salaries	$ 11,625,482	$ 11,921,775	$ 296,293	$ 11,932,519	$ 307,037
Payroll Taxes	651,076	641,983	(9,093)	667,518	16,441
Benefits	1,443,502	1,535,203	91,700	1,634,753	191,251
Retirement Costs	1,010,928	1,137,204	126,276	1,027,262	16,334
Total Personnel Expenses	**$ 14,730,988**	**$ 15,236,164**	**$ 505,175**	**$ 15,262,052**	**$ 531,063**
Meeting Expenses					
Meetings	$ 375,500	$ 375,500	$ -	$ 375,500	$ -
Travel	570,000	537,955	(32,045)	570,000	-
Conference Calls	119,600	83,903	(35,697)	94,800	(24,800)
Total Meeting Expenses	**$ 1,065,100**	**$ 997,358**	**$ (67,742)**	**$ 1,040,300**	**$ (24,800)**
Operating Expenses					
Consultants & Contracts	$ 3,290,966	$ 3,513,672	$ 222,706	$ 3,442,763	$ 151,797
Office Rent	3,091,804	3,087,919	(3,885)	3,335,058	243,254
Office Costs	3,874,198	3,977,329	103,130	4,387,967	513,769
Professional Services	2,287,500	2,265,938	(21,562)	2,386,975	99,475
Miscellaneous	34,500	34,500	-	57,000	22,500
Depreciation	981,159	981,159	-	2,235,443	1,254,284
Total Operating Expenses	**$ 13,560,127**	**$ 13,860,516**	**$ 300,389**	**$ 15,845,207**	**$ 2,285,079**
Total Direct Expenses	**$ 29,356,216**	**$ 30,094,038**	**$ 737,822**	**$ 32,147,559**	**$ 2,791,343**
Indirect Expenses	**$(29,495,094)**	**$ (30,232,916)**	**$ (737,822)**	**$ (32,361,730)**	**$ (2,866,636)**
Other Non-Operating Expenses	**$ 138,878**	**$ 138,878**	**$ -**	**$ 214,171**	**$ 75,293**
Total Expenses (A)	**$ 0**	**$ (0)**	**$ (0)**	**$ 0**	**$ (0)**
Change in Assets	**$ (231,393)**	**$ (38,687)**	**$ 192,706**	**$ (1,067,980)**	**$ (836,587)**
Fixed Assets					
Depreciation	$ (981,159)	$ (981,159)	$ -	$ (2,235,443)	$ (1,254,284)
Computer & Software CapEx	301,000	301,000	-	120,000	(181,000)
Furniture & Fixtures CapEx	-	-	-	-	-
Equipment CapEx	1,175,000	1,175,000	-	890,000	(285,000)
Leasehold Improvements	-	-	-	-	-
Allocation of Fixed Assets	(494,841)	(494,841)	(0)	1,225,443	1,720,284
Inc(Dec) in Fixed Assets (B)	**$ 0**	**$ -**	**$ (0)**	**$ -**	**$ (0)**
TOTAL BUDGET (=A+B)	**$ 0**	**$ (0)**	**$ (0)**	**$ 0**	**$ (0)**
FTEs	**67.45**	**66.16**	**(1.29)**	**67.45**	**-**

Section B – Supplemental Financial Information

Breakdown by Statement of Activity Sections

The following detailed schedules support the consolidated Statement of Activities.

Table B-1 – Operating Reserve and Assessment Analysis

Operating Reserve and Assessment Analysis
Statutory

		Total Reserves	Future Obligation Reserve[1]	Operating Contingency Reserve	System Operator Certification Reserve	CRISP Reserve	Assessment Stabilization Reserve
Beginning Operating Reserves Balance - 1/1/2018		**$ 9,844,365**	**$ 3,015,787**	**$ 3,680,094**	**$ 477,484**	**$ 500,000**	**$ 2,171,000**
Generation or (Use) from 2018 Operations							
From 2018 budgeted operations		$ (634,392)	$ (480,457)	$ (231,393)	$ 77,458	$ -	$ -
From 2018 approved addition/(use) of reserves		-	-	-	-	-	-
Proceeds from financing activities (non-current portion only)	[2]	1,432,000	-	1,432,000	-	-	-
Debt service	[3]	(717,274)	-	(717,274)	-	-	-
Other addition/(use) of reserves	[4]	(1,245,462)	(15,759)	(585,147)	(44,556)	-	(600,000)
Projected Operating Reserves - 12/31/18		**$ 8,679,237**	**$ 2,519,571**	**$ 3,578,280**	**$ 510,386**	**$ 500,000**	**$ 1,571,000**
Required Working Capital and Operating Reserves - 12/31/19		**$ 8,832,757**	**$ 2,039,114**	**$ 3,578,280**	**$ 644,363**	**$ 500,000**	**$ 2,071,000**
Adjustment in funding to achieve required reserve balance		(346,480)	(480,457)	-	133,977	-	-
Penalty sanctions received 7/1/2017 - 6/30/2018 (See Table B-2)		500,000	-	-	-	-	500,000
Less: Assessment Stabilization Reserve Release - Penalties		-	-	-	-	-	-
Total Adjustments to Reserves		**$ 153,520**	**$ (480,457)**	**$ -**	**$ 133,977**	**$ -**	**$ 500,000**
Assessment Reconciliation							
2019 Expenses and Capital Expenditures		$80,049,506					
Less: Assessment Stabilization Reserve Release - Penalties		-					
Adjustment in funding to achieve required reserve balance		133,977					
Less: Other Funding Sources		(9,666,449)					
Less: Proceeds from financing activities (non-current only)		(2,178,667)					
Plus: Debt service		1,110,687					
2019 NERC Assessment		**$69,449,054**					

[1]As further explained in the discussion of the Working Capital Reserve amount in Exhibit D, the Future Obligations Reserve offsets future, non-current liabilities. The calculation of Working Capital and Operating Reserve balances per 2017 audited financials and as projected for 2018 and 2019 is included with the Statements of Financial Position that follow in *Section D - Supplemental Financial Statements.*

[2]Proceeds from financing activities amount is equal to two-thirds of the amount financed or to be financed in the year. See Exhibit D.

[3]Debt Service amount is equal to Annual Payments for Debt Service less Interest Expense. See Exhibit C.

[4]Represents transactions recorded only on the Statement of Financial Position (balance sheet) and do not impact the Statement of Activities (income statement), including recording of capitalized leases, amortization of future obligations, and funding the 457f plan.

Table B-2 – Penalties

Penalty Sanctions

The *NERC Policy – Accounting, Financial Statement and Budgetary Treatment of Penalties Imposed and Received for Violations of Reliability Standard*, as well as § 1107.2 of the ROP, specify that penalty monies received by NERC during the 12 months ended June 30 are to be used in the subsequent budget year to offset assessments. In 2015, the Board approved an updated *Working Capital and Operating Reserves Policy* that was approved by FERC. This updated policy allows NERC, with Board and FERC approval pursuant to § 1107.4 of the ROP, to place penalty funds into an Assessment Stabilization Reserve for use in future years to offset assessments. For the 2019 budget, subject to Board and FERC approval, NERC will deposit penalties collected during the period July 1, 2017–June 30, 2018 into the Assessment Stabilization Reserve. NERC and the Board are also considering a release of $564k from the Assessment Stabilization Reserve to reduce 2019 assessments. The balance held in the Assessment Stabilization Reserve will be used for future assessment offsets.

Allocation Method

Penalty sanctions released from the Asset Stabilization Reserve to offset 2019 assessments will be allocated to the following statutory programs to reduce assessments: (1) Reliability Standards, (2) Compliance Assurance, (3) Compliance Analysis, Organization Registration and Certification, (4) Compliance Enforcement, (5) RASA, (6) Situation Awareness, (7) Event Analysis,(8) Performance Analysis, (9) E-ISAC (including CRISP), and (10) Training and Education. Penalty sanctions are allocated based on the number of FTEs in the program divided by the aggregate total FTEs in the programs receiving the allocation.

All penalties received during the 12-month period ended June 30, 2018 will be detailed in a table provided in the second draft of the 2019 BP&B.

Table B-3 – Outside Funding

Outside Funding Breakdown By Program (Excludes Penalty Sanction)	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget
Reliability Standards			
Workshops	$ 50,000	$ 60,000	$ 10,000
Interest Income Allocation	10,717	17,634	6,917
Total	**$ 60,717**	**$ 77,634**	**$ 16,917**
Compliance Analysis, Registration and Certification			
Interest Income Allocation	$ 6,495	$ 12,162	$ 5,666
Total	**$ 6,495**	**$ 12,162**	**$ 5,666**
Compliance Assurance			
Interest Income Allocation	$ 13,316	$ 24,931	$ 11,616
Total	**$ 13,316**	**$ 24,931**	**$ 11,616**
Compliance Enforcement			
Interest Income Allocation	$ 8,444	$ 15,810	$ 7,366
Total	**$ 8,444**	**$ 15,810**	**$ 7,366**
Reliability Assessment and System Analysis			
Services and Software	$ -	$ -	$ -
Workshops	25,000	25,000	-
Interest Income Allocation	9,743	19,459	9,716
Total	**$ 34,743**	**$ 44,459**	**$ 9,716**
Performance Analysis			
Services and Software	$ 50,000	$ 40,000	$ (10,000)
Interest Income Allocation	6,495	12,162	5,666
Total	**$ 56,495**	**$ 52,162**	**$ (4,334)**
Training, Education, and Personnel Certification			
Testing Fees	$ 540,000	$ 540,000	$ -
Certificate Renewals	650,000	650,000	-
Continuing Education Fees	600,000	600,000	-
Interest Income Allocation	4,060	6,385	2,325
Total	**$ 1,794,060**	**$ 1,796,385**	**$ 2,325**
Event Analysis			
Workshops	$ 40,000	$ 40,000	$ 0
Interest Income Allocation	7,794	13,378	5,583
Total	**$ 47,794**	**$ 53,378**	**$ 5,583**
Situation Awareness			
Interest Income Allocation	$ 3,897	$ 7,297	$ 3,400
Total	**$ 3,897**	**$ 7,297**	**$ 3,400**
E-ISAC			
Third Party Funding (CRISP)	$ 7,324,253	$ 7,456,449	$ 132,196
Workshops	70,000	70,000	-
Interest Income Allocation	24,038	55,782	31,744
Total	**$ 7,418,290**	**$ 7,582,231**	**$ 163,940**
Grand Total	**$ 9,444,253**	**$ 9,666,449**	**$ 222,196**

- Interest Income Allocation – The aggregate $90k increase is the result of higher anticipated interest rates in 2019.
- Third Party Funding (CRISP) – The $132k increase is due to the increase in NERC costs, which are funded equally by participants in CRISP and through assessments.

Table B-4 – Personnel

Personnel	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Salaries	$ 31,791,098	$ 33,960,220	$ 2,169,123	6.8%
Payroll Taxes	1,949,557	2,062,799	113,242	5.8%
Benefits	3,988,886	4,691,914	703,027	17.6%
Retirement	3,239,565	3,435,513	195,949	6.0%
Total	**$ 40,969,105**	**$ 44,150,446**	**$ 3,181,341**	**7.77%**
FTEs	199.28	204.92	5.64	2.8%
Cost per FTE				
Salaries	$ 159,530	$ 165,724	$ 6,194	3.9%
Payroll Taxes	9,783	10,066	283	2.9%
Benefits	20,016	22,896	2,880	14.4%
Retirement	16,256	16,765	509	3.1%
Total	**$ 205,586**	**$ 215,452**	**$ 9,866**	**4.80%**

Below is additional information on the components of personnel expense:

- Salaries – Total salary expense is comprised of base salaries, incentive compensation, deferred compensation, employment agency fees, and temporary office expenses. The 2019 budget for base salaries assumes a 3% increase over actual 2018 base salaries and is inclusive of market adjustments and promotions. The 2019 budget for incentive compensation is based on historical actuals and is comparable to prior years. The 2019 budgets for deferred compensation, employment agency fees, and temporary office expenses are generally consistent with 2018.
- Benefits are budgeted to increase 17.5% based on a 7.5% increase in health and dental premiums, as well as an increase in training expenses to support staff development.
- There have been no changes to NERC's retirement plans.

Table B-5 – Meetings

Meetings	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Meetings	$ 1,071,500	$ 1,071,500	$ 0	0.0%
Travel	2,204,000	2,184,000	(20,000)	-0.9%
Conference Calls	119,600	139,900	20,300	17.0%
Total	**$ 3,395,100**	**$ 3,395,400**	**$ 300**	**0.0%**

Table B-6 – Consultants and Contracts

NOTE: This table has been replaced by Exhibit B – Consultant and Contract Costs

Table B-7 – Rent

Office Rent	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Office Rent	$ 2,819,554	$ 3,122,808	$ 303,254	10.8%
Maintenance	272,250	212,250	(60,000)	-22.0%
Total	**$ 3,091,804**	**$ 3,335,058**	**$ 243,254**	**7.9%**

- The $303k increase in office rent is attributed to facility expansion for the Atlanta office to provide additional meeting space with the goal of reducing future offsite meeting expenses.
- The $60k decrease in maintenance costs is due to a historical trend of lower facility maintenance costs.

Table B-8 – Office Costs

Office Costs	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Telephone	$ 422,387	$ 317,611	$ (104,776)	-24.8%
Telephone Answering Service	2,750	1,200	(1,550)	-56.4%
Internet	383,966	325,460	(58,506)	-15.2%
Office Supplies	190,750	175,700	(15,050)	-7.9%
Computer Supplies	106,100	104,600	(1,500)	-1.4%
Software License and Support*	2,954,942	4,174,234	1,219,292	41.3%
Subscription and Publications	194,970	228,420	33,450	17.2%
Dues	66,911	69,611	2,700	4.0%
Postage	15,540	10,540	(5,000)	-32.2%
Express Shipping	26,992	28,992	2,000	7.4%
Copying	115,842	117,642	1,800	1.6%
Audio/Visual and Hardware Lease**	640,336	752,529	112,193	17.5%
Equipment Repair/Service Contracts	132,497	132,497	-	0.0%
Bank Charges	25,000	25,000	-	0.0%
Merchant Card Fees	86,100	86,100	-	0.0%
Total	**$ 5,365,084**	**$ 6,550,137**	**$ 1,185,053**	**22.1%**

**Combined Software and Maintenance/Service Agreement accounts to streamline accounting activities*

***Combined Audio/Visual and Hardware Lease accounts to streamline accounting activities*

- Telephone – The $105k decrease is primarily related to lower conference call expenses due to a change in service providers.
- Internet – The $59k decrease is the result of cost reductions through vendor negotiation.
- Software License and Support – The $1.2M increase is primarily the result of annual software subscription and support costs of $589k for the new CMEP software tool, and a higher historical trend than previously budgeted in non-capital software and support expenses. The increase in 2019 is partially offset by a lower capital expenditure budget in NERC software costs.
- Subscriptions and Publications – The $33k increase is primarily due to additional subscription resource needs in the Policy & External Affairs and Event Analysis departments.
- Audio/Visual and Hardware Lease – The $112k increase is the result of anticipated leases of new computer and hardware equipment.

Table B-9 – Professional Services

Professional Services	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Independent Trustee Fees	$ 1,237,500	$ 1,289,375	$ 51,875	4.2%
Trustee Search Fees	100,000	100,000	-	0.0%
Outside Legal	595,500	645,500	50,000	8.4%
Lobbying	72,000	72,000	-	0.0%
Accounting and Auditing Fees	128,000	128,000	-	0.0%
Insurance Commercial	231,000	225,000	(6,000)	-2.6%
Outside Services	173,500	177,100	3,600	2.1%
Total	**$ 2,537,500**	**$ 2,636,975**	**$ 99,475**	**3.9%**

- Independent Trustee Fees – The $52k increase is the result of the addition of a trustee per the Board's decision to search for the new trustee in 2018 instead of 2019. This decision was made to reduce the number of trustee searches that would need to be conducted in 2019 as a result of the coinciding term expirations of two current trustees.
- Outside Legal – The $50k increase primarily due to support costs for the E-ISAC long-term strategy.

Table B-10 – Miscellaneous

Miscellaneous Expenses	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Miscellaneous Expense	$ 7,000	$ 7,000	$ -	0.0%
Employee Rewards and Recognition*	28,000	50,500	22,500	80.4%
Community Responsibility & Employee Engagement	4,500	4,500	-	0.0%
Total	**$ 39,500**	**$ 62,000**	**$ 22,500**	**57.0%**

** Includes costs associated with the year-end employee recognition event*

Table B-11 – Other Non-Operating Expenses

Other Non-Operating Expenses	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Property and Other Tax Expense	$ 50,000	$ 120,000	$ 70,000	140.0%
Interest Expense	88,878	94,171	5,293	6.0%
Total	**$ 138,878**	**$ 214,171**	**$ 75,293**	**54.2%**

- Property and Other Tax Expense – The $70k increase is due to federal excise taxes for parking and mass transit expenses, which is a new expense item and is based on recent changes to federal tax laws.
- Interest Expense – Budgeted interest expense is calculated based on expected draws on the capital financing loan. Refer to *Exhibit C – Capital Financing* for more detailed information related to debt repayment and the interest expense calculation.

Table B-12 – Fixed Assets

Fixed Assets	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
Depreciation	$ (1,594,299)	$ (3,446,022)	$ (1,851,724)	116.1%
Computer & Software CapEx	2,549,000	3,488,000	939,000	36.8%
Furniture & Fixtures CapEx	-	-	-	0.0%
Equipment CapEx	1,175,000	890,000	(285,000)	-24.3%
Leasehold Improvements	150,000	400,000	250,000	166.7%
Total	**$ 2,279,701**	**$ 1,331,978**	**$ (947,724)**	**-41.6%**

As discussed in the *Introduction and Executive Summary*, expenditures for fixed assets, excluding the reversal of depreciation expense, are budgeted to be $904k more in 2019 compared to 2018. This increase is primarily due to increased expenditures on ERO Enterprise software projects and leasehold improvements for the E-ISAC.

Table B-13 – 2019–2020 Projections

NOTE: Refer to the Executive Summary* section on *page 18

Section C – Non-Statutory Activity

NERC has no non-statutory activities.

Section D – Supplemental Financial Statements

NERC statement of financial postion and landscape of activities will be provided in the second draft of the 2019 BP&B.

Exhibit A – Application of NERC Section 215 Criteria

DISCUSSION OF HOW THE NERC MAJOR ACTIVITIES
IN THE 2019 BUSINESS PLAN AND BUDGET
MEET THE NERC WRITTEN CRITERIA FOR DETERMINING WHETHER A
RELIABILITY ACTIVITY IS ELIGIBLE TO BE FUNDED UNDER
FEDERAL POWER ACT SECTION 215

Exhibit will be provided in the second draft of the 2019 BP&B.

Exhibit B – Consultant and Contract Costs

Consultants & Contracts	2018 Budget	2019 Budget	Increase (Decrease)
Reliability Standards			
Standards Development Support		$ 50,000	$ 50,000
Total		**$ 50,000**	**$ 50,000**
Compliance Assurance			
Risk-Based Compliance Monitoring Implementation	$ 50,000	$ 50,000	$ -
Total	**$ 50,000**	**$ 50,000**	**$ -**
Reliability Assessment and System Analysis			
Reliability Effects of GMD	$ 100,000	$ 200,000	$ 100,000
Reliability Consulting Support	$ 425,000	$ 425,000	$ -
Total	**$ 525,000**	**$ 625,000**	**$ 100,000**
Performance Analysis			
GADS/TADS/DADS	$ 572,030	$ 653,565	$ 81,535
Total	**$ 572,030**	**$ 653,565**	**$ 81,535**
Situation Awareness			
Reliability Tools	$ 600,595	$ 614,110	$ 13,515
Secure Alerting System	$ 96,000	$ 98,880	$ 2,880
SAFNR - Phase II	$ 523,900	$ 493,000	$ (30,900)
Communication Network	$ 75,000	$ 75,000	$ -
Total	**$ 1,295,495**	**$ 1,280,990**	**$ (14,505)**
E-ISAC			
CIPC Support	$ 33,000	$ 33,000	$ -
GridEx Support	$ 142,000	$ 550,000	$ 408,000
Program-Level Capabilities	$ 770,000	$ 725,000	$ (45,000)
Software and Services	$ 105,200		$ (105,200)
Portal Improvement		$ 462,500	$ 462,500
Events and Outreach	$ 50,000	$ 50,000	$ -
CRISP	$ 6,291,594	$ 6,457,500	$ 165,906
Total	**$ 7,391,794**	**$ 8,278,000**	**$ 886,206**
Personnel Certification			
System Operator Testing Expenses	$ 58,500	$ 62,000	$ 3,500
System Operator Examination Development	$ 50,000	$ 50,000	$ -
Job Task Analysis	$ 42,000		$ (42,000)
Database License	$ 25,200		$ (25,200)
SOCCED Database Improvements	$ 75,000	$ 50,000	$ (25,000)
Total	**$ 250,700**	**$ 162,000**	**$ (88,700)**
Training and Education			
Continuing Education Program	$ 133,200	$ 108,000	$ (25,200)
ERO Enterprise Learning Portal	$ 103,150	$ 117,000	$ 13,850
ERO Enterprise and Industry Course Development	$ 76,850	$ 125,000	$ 48,150
NERC Staff Technical Training	$ 35,000	$ 35,000	-
Total	**$ 348,200**	**$ 385,000**	**$ 36,800**
General and Administrative			
Communications Support	$ 20,000	$ 20,000	$ -
Executive Consulting	$ 80,000	$ 280,000	$ 200,000
Total	**$ 100,000**	**$ 300,000**	**$ 200,000**
Information Technology			
ERO Data Analytics	$ 1,277,966	$ 1,307,763	$ 29,797
Applications Enhancements, Consulting, and Help Desk Support	$ 846,000	$ 670,000	$ (176,000)
Total	**$ 2,123,966**	**$ 1,977,763**	**$ (146,203)**
Human Resources			
Training and Development	$ 400,000	$ 400,000	$ -
Compensation Consulting	$ 175,000	$ 225,000	$ 50,000
Employee, Industry, and Board Surveys	$ 40,000	$ 40,000	$ -
HR Consulting Services	$ 25,000	$ 25,000	$ -
Total	**$ 640,000**	**$ 690,000**	**$ 50,000**
Finance and Accounting			
Internal Controls and Outside Auditor Consulting Support	$ 220,000	$ 300,000	$ 80,000
Finance and Accounting Support	$ 207,000	$ 175,000	$ (32,000)
Finance and Accounting	**$ 427,000**	**$ 475,000**	**$ 48,000**
Total Consultants & Contracts	**$ 13,724,185**	**$ 14,877,318**	**$ 1,153,133**

Exhibit C – Capital Financing

The company initiated a capital financing program in January 2014 as a funding source for major software application development projects that primarily benefit the ERO Enterprise. The total size of the original non-revolving credit facility was $7.5M and was used to finance a portion of NERC's capital expenditures (including IT hardware and software application development costs) made through December 2016. A similar non-revolving credit facility was closed in November 2016, totaling $5.0M, and is available to finance certain capital expenditures made from January 2017 to December 2019. The interest rate for both credit facilities is floating and equal to LIBOR plus 275 basis points. Authorized annual borrowings under the facilities are limited to the amount approved by the Board and FERC in each year's BP&B. Borrowings under the credit facilities are amortized over a three-year period, and can be prepaid without penalty.

As further discussed in the *Introduction and Executive Summary* and set forth in the table below, NERC has a 2019 proposed capital budget of approximately $4.8M, of which it is proposing to finance $3.3M.

NERC Capital Budget	Budget 2018	Budget 2019	Variance 2019 Budget v 2018 Budget	Variance %
ERO Application Development	$ 2,148,000	$ 3,268,000	$ 1,120,000	52.1%
Hardware (storage, servers)	805,000	565,000	(240,000)	-29.8%
Other Equipment	370,000	425,000	55,000	14.9%
Disaster Recovery	100,000	-	(100,000)	-100.0%
NERC Software Licenses	301,000	120,000	(181,000)	-60.1%
Leasehold Improvements	150,000	400,000	250,000	166.7%
Total	**$ 3,874,000**	**$ 4,778,000**	**$ 904,000**	**23.3%**

In the 2019 budget, NERC plans to finance $3,268,000 for ERO Enterprise application development projects. Tables showing projected year-end outstanding debt and the future annual payments for debt service will be provided in the second draft of the 2019 BP&B.

Exhibit D – Working Capital and Operating Reserve Amounts

In September 2015, FERC approved NERC's proposed amendments to its *Working Capital and Operating Reserve Policy*, which had been approved by the Board. A number of changes were made to the policy, including:

- Clarifying the definition of working capital to represent funding needed for cash flow purposes due to the timing of the receipt of funds and the payment of expenses.
- Creating four separate categories of operating reserves:
    1. A **Future Obligation Reserve** for funds being held to satisfy obligations that will be settled in a future year. Examples include leases, certain contracts, and credit agreements. These reserves were previously included within the definition of working capital, but are more accurately classified as a form of operating reserve.
    2. Continuation of a separate category of reserves for the Operator Certification Program called the **System Operator Certification Reserve**.
    3. Elimination of the Known and Unforeseen Contingency categories of operating reserves and creating a single category of contingency reserves called the **Operating Contingency Reserve**.
    4. Creation of a separate category of reserves for CRISP called the **CRISP Reserve**.

Working Capital

Based on its 2018 cash flow projection and taking into account the historic manner in which NERC's assessments have been billed and paid, NERC does not anticipate needing access to working capital in 2019 to meet monthly cash flow needs. While individual reserve categories are increasing and decreasing based on operating needs and uses, the budget in total does not reflect additional net funding for reserves. In the unlikely event NERC experiences a temporary cash flow shortage, it has the ability to either request authorization from the FAC and Board to temporarily access operating contingency reserve funds, or draw on its $4M line of credit, as long as NERC is in compliance with the covenants under its bank credit agreement.

Operating Reserves

Total operating reserves are budgeted to be $6.8M at December 31, 2019 among all four categories, or $6.3M excluding the $500k CRISP Reserve. The Future Obligation Reserve is budgeted to be $2.0M and is primarily funds held to offset future liabilities under lease agreements for the Atlanta and Washington, DC, offices. System Operator Certification Reserves are budgeted at $644k, and the Operating Contingency Reserve is budgeted for $3.6M. The CRISP Reserve, budgeted at $500k, is held pursuant to the terms of the Master Services Agreement between NERC and participating utilities, which calls for a separate third-party funded reserve established to fund certain contingencies in connection with CRISP.

Assessment Stabilization Reserve

In addition to the foregoing reserves, the amended policy also provides for an Assessment Stabilization Reserve. The goal of the Assessment Stabilization Reserve is to mitigate assessment volatility and have percentage changes in annual assessments track, within a reasonable band, percentage changes in the company's total annual budget, with the total budget reflecting prudent fiscal discipline and good stewardship of resources. Assessment stabilization funds will be used when available to help stabilize assessments and mitigate year-to-year swings in assessments. Those swings primarily result from the year-to-year variations in collections of penalty funds to be applied to offset assessments, but could also result from other factors like surplus funds available from a prior period, the need to replenish the Operating Contingency Reserve, or significant but relatively short-term operating or capital spending needs. Subject to Board and FERC approval, NERC will deposit any penalties collected during the period July 1, 2017–June 30, 2018, into the Assessment Stabilization Reserve. NERC and the Board are also considering a release of $564k from the Assessment Stabilization Reserve.

Exhibit E – E-ISAC Long-Term Strategy

Executive Summary

The Electricity Information Sharing and Analysis Center (E-ISAC), operated by the North American Electric Reliability Corporation (NERC), executed a significant improvement initiative over the past two years based on findings and recommendations developed by the Electricity Subsector Coordinating Council (ESCC) in 2015. Looking forward, the electricity industry would like the E-ISAC to become an indispensable resource for security information sharing and analysis, and to be the centerpiece for building a highly engaged community of security professionals.

To carry forth this vision, the E-ISAC must undergo continuous improvement and evolution that reflects the changing threat landscape, changing technologies and business processes inside the industry, and changing customer expectations for a highly reliable and secure electricity infrastructure that is increasingly more integrated with insecure infrastructures such as the public Internet. This will require additional resources for people, technology, and facilities above what has been budgeted in previous years.

This strategic plan builds on the ESCC's earlier recommendations and discusses improvements needed in 2017 to address current threats, a look at the mid-term range of 2018-2022 to address emerging threats, and what the E-ISAC might look like beyond 2023 if the forecasted issues continue to develop.

The plan was developed with guidance from the ESCC and from NERC leadership. It recognizes the need for sound fiscal planning, recognizes the growing threats to the grid from human and cyber actors, and highlights the need for a more robust security information sharing and analysis capability within NERC.

At a recent planning session with C-level executives, one utility CEO said he wanted to "transform the EISAC into an intelligence collecting and analytical capability that industry literally cannot do without," which resonated strongly among the other executives. To achieve this goal we must get the E-ISAC to a maturity level where industry completely trusts it to gather, hold, analyze, and distribute highly sensitive security information.

Specific financial projections, technology requirements, staffing, and facility improvements are being developed and will be incorporated in the NERC strategic plan and the NERC business plan and budget.

Background

The Electricity Information Sharing and Analysis Center (E-ISAC) is operated by the North American Electric Reliability Corporation (NERC).[36] It was established by NERC at the request of the U.S. Department of Energy in 1999 to serve as a focal point for voluntary information sharing within the electricity subsector. By 2006, the ISAC was widely used in the subsector for collecting, analyzing, and distributing voluntarily-shared security information and was a key component of NERC's overall electric reliability mission. NERC's Board of Trustees oversees the budget and activities of the E-ISAC in the same manner as other NERC divisions.

NERC assumed the role of the Electric Reliability Organization (ERO) in 2006 and began a multi-year effort to develop enforceable reliability and security standards for owners, operators, and users of the Bulk-Power System. As the standards were completed and compliance monitoring began, the ISAC remained the place where security incidents were reported, but the voluntary nature of reporting from electricity entities shifted towards mandatory reporting from entities required to be compliant with NERC's Critical Infrastructure Protection (CIP) standards. By 2014, voluntary sharing with the E-ISAC had greatly diminished in favor of mandatory reporting, but the desire

[36] Initially called the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the name was changed in September 2015 to the Electricity Information Sharing and Analysis Center (E-ISAC) as part of a rebranding and role-clarification initiative.

for voluntary sharing within the subsector remained strong. The following year a perceived problem of internal NERC cross-sharing of security information was addressed when NERC implemented the employee code of conduct that bars voluntarily shared security information from being forwarded to NERC's compliance and enforcement teams. Also in 2015 the E-ISAC finished a separation project that includes physical and electronic barriers to protect the information voluntarily shared by industry members.

In late 2014, the Electricity Subsector Coordinating Council (ESCC) initiated a strategic review of the E-ISAC. In June 2015, the ESCC published its key findings and recommendations, which fell into four major areas of improvement for the E-ISAC:

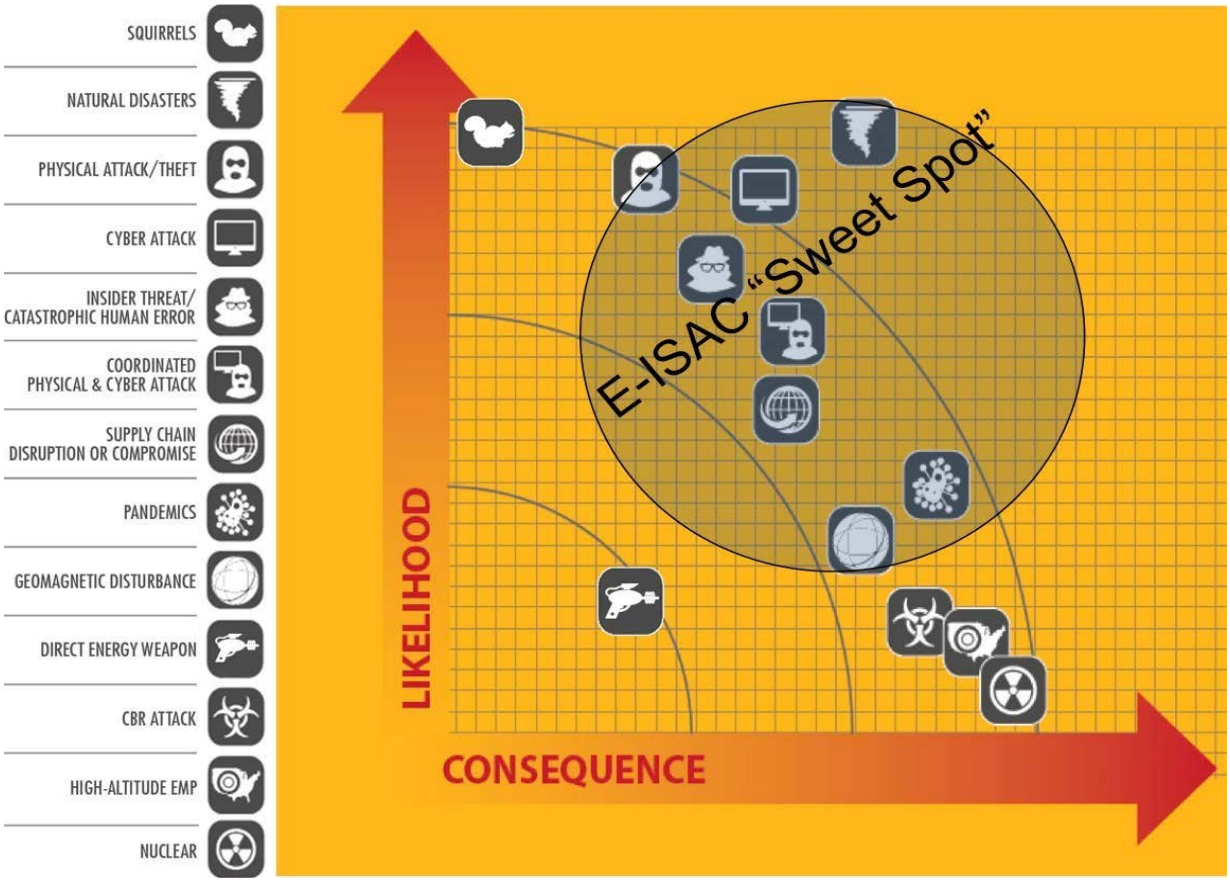
- Strengthen the governance structure and processes to increase effectiveness and responsiveness
- Improve the quality and value of the products by identifying member needs and expectations
- Advance the analysis capabilities by continuing to upgrade operational and staff capabilities
- Advance the information collection capabilities through enhanced member engagement, better tools or sensors, and an improved portal

A C-level advisory team from the ESCC (the Member Executive Committee, or MEC) was established in 2015 to help enable the implementation of the ESCC's recommendations, which included a new vision for the E-ISAC to become the electricity industry's leading, trusted source for analysis and sharing of security information. As of April 2017, much progress has been made toward realizing this vision and now we look forward to the next five years and beyond while asking the question, "how do we transform the E-ISAC into an intelligence collecting and analytical capability industry cannot do without?" To begin this process, the following section looks back at known threats and ahead at the anticipated evolving nature of future threats targeting the electricity industry.

The Changing Threat Landscape

A study conducted for the ESCC by the Chertoff Group in 2014[37] found that a range of threats target the electric power grid. These threats can be approximately related to each other by using a likelihood versus consequence plotting. We feel that the E-ISAC's "sweet spot" is roughly along the 45-degree line as depicted in the graphic below.

[37] "Addressing Dynamic Threats to the Electric Power Grid Through Resilience" https://www.chertoffgroup.com/files/docs/Addressing-Dynamic-Threats.compressed.pdf



Industry by itself cannot protect the grid from all hazards, and likewise neither can the government. A strong partnership between industry and government for security is required, and in fact has been in place for many years. At the center of this partnership is the ESCC, which serves as a bridge between the public and private sectors for strategic security policy coordination and to develop unity of messaging during a crisis. In addition, timely and actionable information sharing, collaboration, and analysis are the cornerstones of good security practices within the electricity industry. The E-ISAC's role is to facilitate voluntary sharing and collaboration, and to provide unique insights into emerging security issues that are affecting the sector. In January 2017 the E-ISAC and the MEC met in person to discuss the future of the E-ISAC relative to changing threats, changing industry dynamics, and a changing environment. While physical threats resulting in theft, vandalism, disruption, or destruction will always be present, the group recognized that cyber threats and other types of threats are evolving and will require adaptive change throughout industry and especially with respect to the E-ISAC. The group agreed that future threats industry needed to monitor and mitigate included:

- Near-term (0–2 years)
  - Nation state threats, advanced persistent threats, the Internet of Things (IoT), Distributed Denial of Service (DDoS) attacks, and ransomware
  - Data breaches and intellectual property theft
  - Insiders, physical damage, coordinated attacks, and third-party risks
- Mid-term (3–5 years)
  - Increased reliance on gas generation
  - Distribution system vulnerabilities via networked control systems

  - Growth of demand response technologies with low security
  - Distributed energy resources
  - Reliability of communications networks
- Long-term (5–10 years)
  - Higher replacement rate of components and systems
  - Increased cost of operations due to higher security costs
  - Ability to run manually might be lost
  - Computers attacking computers

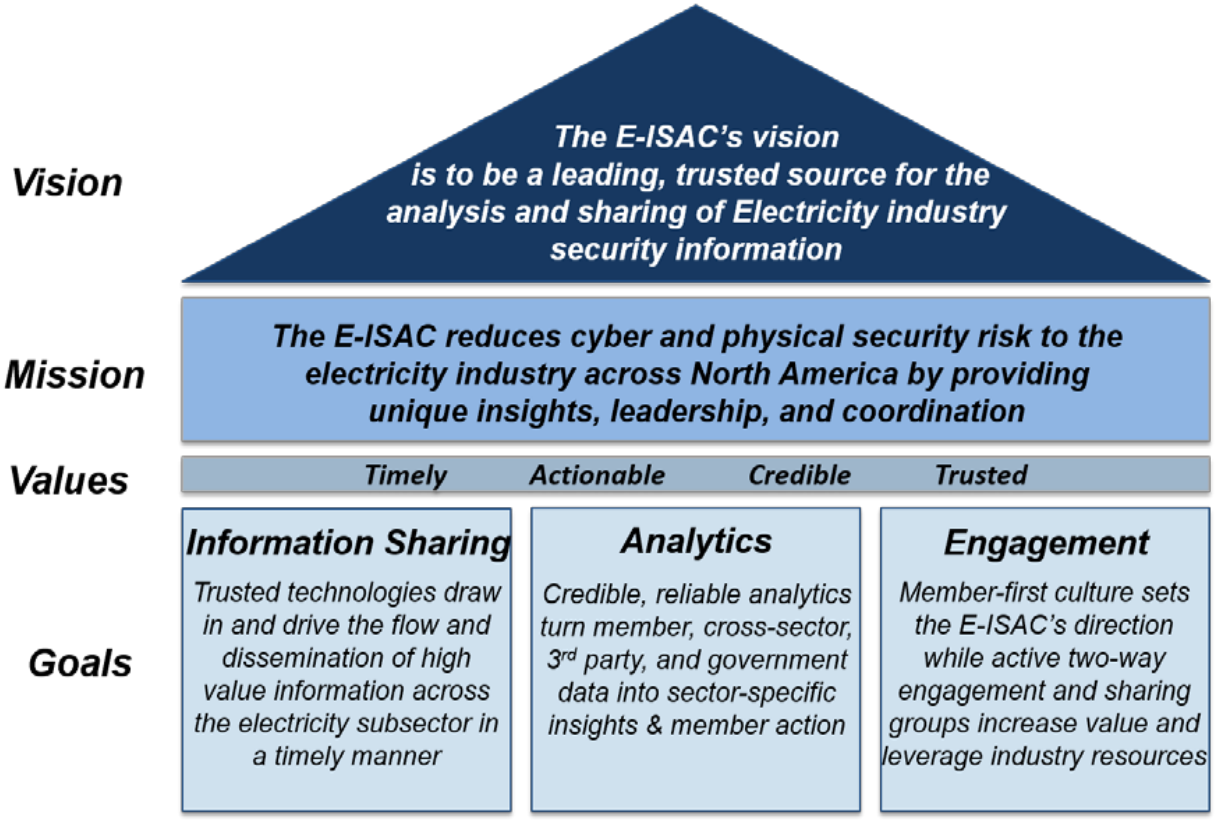
The remainder of this plan discusses improvements needed in 2017 to address current threats, a look at the mid-term range of 2018–2022 to address emerging threats, and what the E-ISAC might look like beyond 2023 if the forecasted issues continue to develop.

The Need for a Strategic Plan

Given that quite a bit of work was accomplished over the past two years to improve the E-ISAC, it is reasonable to ask why a long-term strategic plan is needed. Looking externally, there are three primary drivers:

- Security threats continue to evolve and become more dangerous
  - Ukraine, IoT, and ransomware attacks are indicators
  - Geopolitical tensions and changing societal trends make North America a target
- Customer expectations for highly reliable energy continue to increase
  - Electricity entities need to be more agile and responsive to real-time risks
  - Rapid technology changes also increase the risk landscape
- More robust understanding and measurement of grid resiliency and security
  - Need new tools for collecting and analyzing grid security metrics data

Since the publication of the ESCC's strategic review in 2015, the E-ISAC has solidified vision, mission, values and goals statements as shown in the graphic below. The three "goals" columns represent parts of a rising spiral of membership engagements: bringing in more information improves the analytical process, which in turn drives more engagement, which then brings in more information, which improves analytics, and so forth.

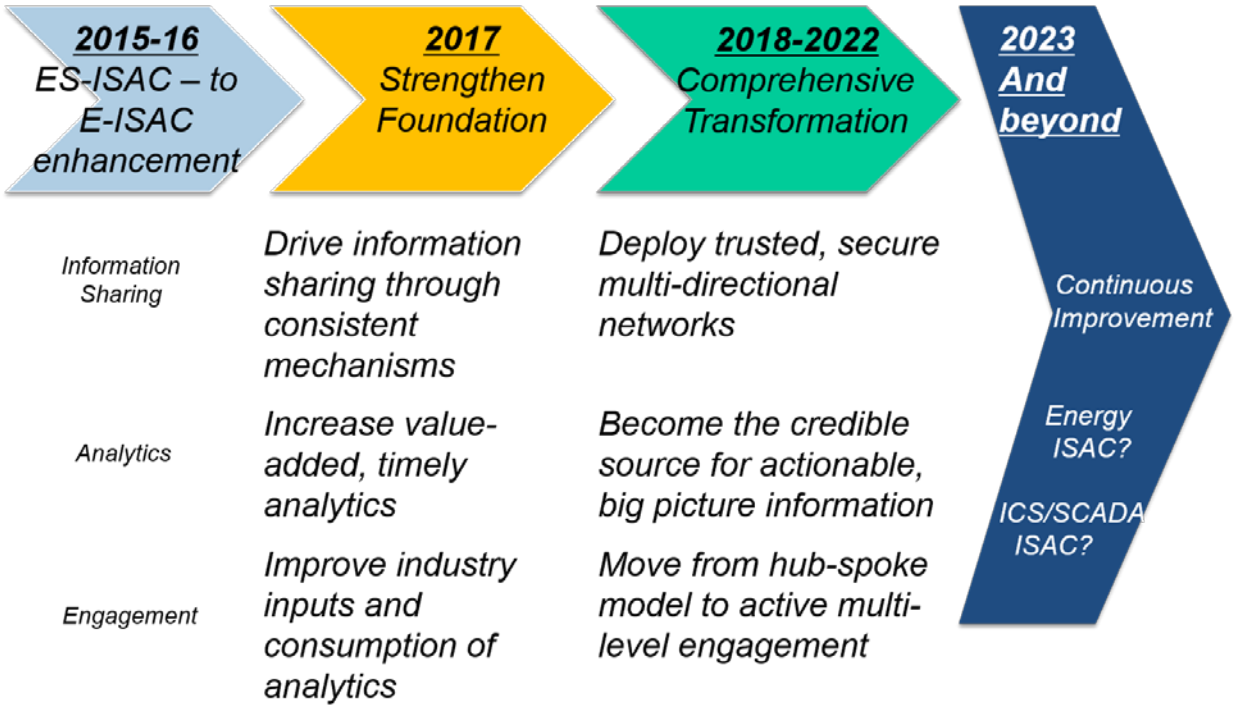


This process takes the E-ISAC to new levels as it gets better at information collection, analysis, and dissemination and represents the core capabilities of the E-ISAC. The MEC and the E-ISAC developed a related strategy for the improvement of the E-ISAC's products and services that builds upon the pillars shown in the graphic above, and is working on a technology roadmap in partnership with NERC's Information Technology team that also follows this method. Both of these more tactical plans support the goals and objectives of the E-ISAC's long-term strategic plan.

Transforming the E-ISAC: 2017 and Beyond

In the coming years, NERC should build on the foundation of the 2015 ESCC recommendations, and position the E-ISAC to provide more robust security information for better understanding of security weaknesses and strengths across the ERO. By addressing the three primary drivers outlined above, NERC can transform the E-ISAC into a world-class intelligence collecting and analytical capability for the electricity industry. To accomplish this, the E-ISAC must achieve a maturity level where industry completely trusts it to gather, hold, analyze, and distribute highly sensitive security information, with no fear that information voluntarily submitted to the E-ISAC would ever be used for a compliance enforcement action or investigation.

As we strengthen the foundation built over the past two years, the E-ISAC should undertake a comprehensive multi-year transformation to build capabilities that include trusted, secure, multidirectional networks and a movement from a hub/spoke model to a very active multi-level engagement. The E-ISAC strives to be the industry's most credible source for actionable, big picture information. This roadmap is illustrated in the graphic below.



2015 and 2016 were foundation-building years, set in motion by the ESCC strategic review and the publication of the findings and recommendations. In 2015, NERC implemented an employee code of conduct, completed a physical and logical separation of the E-ISAC from other parts of NERC, hired strategic leadership and key industry experts, and rebuilt the organization with new internal functional groups. Also that year, the name was changed from the ES-ISAC to the E-ISAC and new logos, color schemes, and branding were launched. In 2016, the old web portal was upgraded with the intention of setting in motion a completely new platform capability that will launch later in 2017. Over the past two years, membership engagement and information sharing grew rapidly, new products and services were launched, and the third Grid Security Exercise (GridEx III) was successfully administered by the E-ISAC. The impact of these initial changes on the E-ISAC's capability to respond to real-world incidents was validated by the Ukraine grid attacks in December 2015, denial of service attacks from Internet of Things (IoT) devices in October 2016, and the second Ukraine event along with the Grizzly Steppe incident at the end of December 2016.

As was pointed out frequently in the past two years, the "IS" and the "A" in "ISAC" define the two primary strategic themes that must be in place for the organization to be successful. In 2017, the E-ISAC is deploying new information sharing and analysis tools such as the Cyber Automated Information Sharing System (CAISS) and an Event Visualization Tool (EVT) to increase the speed and ease of sharing cyber threat information. While the Cybersecurity Risk Information Sharing Program (CRISP) has enhanced visibility and understanding of cyber threats for the electricity industry, processing classified information takes time. As information comes in from CRISP sensors and goes to the Pacific Northwest National Laboratory, the E-ISAC will leverage a new unclassified data storage and analytics capability inside the E-ISAC so that more actionable information can be sent to industry on a timelier basis. Later this year we anticipate that alerts and technical information will flow securely between CAISS and CRISP in our efforts to expand our data collection beyond the current participant pool and to achieve a more comprehensive picture of industry threats than we have today.

The major technical effort in 2017 is a planned replacement of the current web portal with a new "platform" that will enable automatic information sharing, the creation of private discussion groups, data visualization, and many other features that the E-ISAC's members requested. To support the new tools and the needs of the sector,

additional analysts will be hired in 2017. In addition, new partnerships are envisioned with organizations like the Computer Emergency Response Team Coordination Center (CERT/CC), and at the end of 2017, the E-ISAC will host the GridEx IV. In mid-April 2017, the internal structure of the E-ISAC was modified to align the staff to better serve the industry. There are now two major groups—one focused on operations and analysis and the other on programs and member engagement. Some minor facility improvements are also planned for 2017.

Looking forward, the next five years (2018-2022) will focus on transforming the E-ISAC into a world-class intelligence collecting and analytical capability for the electricity industry. To achieve this goal, the E-ISAC should increase its capability to collect security intelligence; increase the number of specialized analysts; acquire additional data storage, management, and sharing technologies; and increase the E-ISAC's access to classified networks and facilities.

New Intelligence Collection – To Support Better Unclassified Information Sharing

Some new collection capabilities coming online in 2017 such as CAISS and the Department of Energy's CYOTE project will bring additional intelligence, but the E-ISAC should also consider more active monitoring of public and private networks for new threats, perhaps collecting data from sensors in Operational Technology (OT) networks, and increasing the ability to monitor social media and other open sources. Some of that new collection could be done by others as a service that the E-ISAC would pay for.

Access to Classified Networks and Facilities – To Improve Sharing of Highly Sensitive Information

While the majority of the E-ISAC's staff hold US government security clearances, the facility inside of NERC operates at the unclassified level. This requires E-ISAC staff to travel to government facilities in order to view and analyze classified data. On the industry side, very few entities have access to classified facilities and most do not have staff with appropriate clearances. To support the strategic goal of better information sharing, both the E-ISAC and industry members should have increased access to classified data and classified information sharing networks. Relationships with government partners need to be leveraged to make valuable classified data and analysis rapidly available to asset owners and operators.

More Analysts – To Improve the E-ISAC's Analytical Capabilities

The E-ISAC should hire technical analysts with specializations in fields such as industrial control system security, end-point (host) security, network security, cloud security, and penetration testing. Over the next three to five years an estimated ten or more analysts should be hired at a rate of two or three per year so that the annual increase of NERC's budget is minimized.

Acquisition of New Technologies – To Improve Industry Engagement

As more data is collected, the E-ISAC should acquire additional data storage, management, and sharing technologies. These technologies must be as secure as possible, given that the risk of a targeted data breach will increase as the E-ISAC improves its capability to give early warning to industry about threats and vulnerabilities discovered via data analysis. Specific technologies needed in the next five years include event visualization via the new platform, predictive analysis based on artificial intelligence, real-time threat feeds to members, a customized platform experience for each user, and federated information sharing.

Beyond 2023 security challenges will continue to expand, requiring additional resources and perhaps a different relationship across the energy industry. Due to commonality of threats across all energy companies, rapid growth of vulnerable control systems, and a convergence of lines of business within the industry, we must consider whether or not the E-ISAC should remain focused only on electricity, or if it should expand to include all energy owners/operators (electricity, gas, oil, and natural gas).

Other items to consider beyond 2023 include the size and location of the E-ISAC facility and potential partnerships with the research community. Due to limitations of the NERC budget, some of these new capabilities would need outside funding from the government or perhaps grants from large industry companies.

Other MEC Guidance

Several questions were presented to the MEC membership about the long-term future of the E-ISAC. Most of the questions were answered in the discussion paragraphs above. The remaining questions not previously discussed and the MEC's summarized responses are below.

Should the E-ISAC move to 24/7 operations?

Not immediately but the decision should be based on changing situations and activity levels. This response is driven by the reality of the cost for the additional staff, and by the reality that very little data is submitted to the E-ISAC for analysis outside of normal business hours. But, as the E-ISAC's capabilities and data collection grow, there will likely be a point in the next 3-5 years when it might be necessary to move to round-the-clock operations.

What is the E-ISAC's relationship with other ISACs?

There is concern that other ISACs (the Financial Services ISAC, or FS-ISAC, is a recent example) will attempt to recruit electric utilities to pay for special analytical services in order to cover expanding costs. The consensus view of the MEC is that the E-ISAC should not discourage members from taking advantage of services offered by other ISACs, and should try to learn about those new capabilities with an eye towards developing them organically within the E-ISAC when appropriate. Services offered by other ISACs should be viewed as additional intelligence sources. Additionally, the E-ISAC should develop stronger information sharing partnerships with other ISACs and increase the level of cross-sector engagement.

Should the E-ISAC have an international relationship?

The E-ISAC, as part of NERC, currently has members in Canada and Mexico. The MEC recommended that the E-ISAC consider establishing formal information sharing relationships with other countries such as Japan or the United Kingdom. Because no other countries are interconnected with the North American grid beyond the US, Canada, and Mexico, any future information sharing relationship with entities in other countries would be at a very high level and must preserve the privacy of North American entities that are voluntarily sharing with the E-ISAC.

Should the E-ISAC accept funding from sources beyond NERC assessments?

Government funding may be necessary to cover costs of the recommended expansions of technical capabilities, staff, and facilities. MEC members cautioned about any potential "attached strings" that come with government grants. Beyond 2018, some member companies have expressed interest in a model like CRISP where companies can pay for additional services, or perhaps moving to a tierbased pricing model.

Conclusion and Next Steps

The next several years present an opportunity to transform the E-ISAC into a world-class intelligence collecting and analytical capability for the electricity industry; and an opportunity to support NERC's overall initiatives to better understand the current security posture of the North American grid. As threats, technologies, and business process change, the E-ISAC, in order to be as valuable as it can to the industry, must evolve to a maturity level where industry completely trusts it to gather, hold, analyze, and distribute highly sensitive security information. Specific financial projections, technology requirements, staffing, and facility improvements are being developed and will be incorporated in the NERC strategic plan and the NERC business plan and budget.

Towards this transformation, for the near term (remainder of 2017 and all of 2018), the E-ISAC plans to:

- Hire additional analysts
- Increase the in-house data storage and analysis capabilities
- Grow the CRISP and CAISS programs
- Deliver a world-class information sharing platform well before GridEx IV
- Grow membership engagement via the new platform
- Increase engagement with other ISACs and information sharing partners
- Increase engagement with Canada and Mexico
- Provide higher quality grid security metrics data to support NERC's data collection initiatives

Attachment
Expanding E-ISAC Operations to Include 24x7 Onsite Operations

At the request of the ESCC's MEC, the E-ISAC evaluated the benefits of and requirements for expanding operations to include certain 24x7 onsite capabilities. The purpose of this document is to outline: (1) the value of expanding the E-ISAC's operations to include 24x7 on-site capabilities; (2) a recommendation as to the level of 24x7 onsite capabilities the E-ISAC should implement; and (3) the staffing and other requirements necessary to implement such capabilities.

This document is organized as follows:

- *Section I* provides an executive summary of the E-ISAC's proposal for expanding its operations to 24x7 onsite capabilities.
- *Section II* provides an overview of the E-ISAC's existing organization structure, hours of operation, and staffing levels.
- *Section III* discusses the value of expanding E-ISAC operations to include 24x7 onsite capabilities.
- *Section IV* provides the E-ISAC's proposal with respect to the level of 24x7 capabilities it should offer.
- *Section V* discusses staffing requirements for expanded operations.

Section I: Executive Summary

As discussed further below, the E-ISAC recommends expanding its operations to include certain 24x7 onsite capabilities. Specifically, the E-ISAC would incrementally expand its operations to have one to two E-ISAC personnel onsite at all times to monitor data feeds, respond to member inquiries, and conduct physical and cyber security analysis. 24x7 onsite capabilities could provide significant benefits to members, including (1) timely analysis and information sharing regarding developing physical or cyber security incidents that are discovered or occur outside of normal hours, and (2) the continued development of actionable intelligence during the overnight and weekend hours to enhance industry's preparation for, and response to, any potential physical or cyber security threat or incident.

As the value of expanding E-ISAC operations to include 24x7 capabilities depends, in large part, on increasing the flow of data into the E-ISAC to warrant the additional resources, the E-ISAC recommends accomplishing the expansion to 24x7 onsite capabilities in stages through 2020. Using a phased approach would (1) allow the expansion to 24x7 onsite capabilities to move in parallel with the E-ISAC's plans to increase data flow and deploy additional analytical tools and capabilities, and (2) provide the E-ISAC the ability to reassess the timing of additional projected resources needs on an annual basis during its budget approval process based on data flow and work demands.

The E-ISAC proposes that during 2019, the E-ISAC expand its Monday-Friday operations from 6:00 a.m.-6:00 p.m. to a full 24x5 (minus weekends and holidays), with one watch officer assigned to each after-hours period (see Table 1). In 2020, the E-ISAC proposes to move to a full 24x7 operations by adding onsite staff during weekends and holidays. This proposed plan and resources needs for future years (beyond 2020) will continue to be subject to review and approval in the context of NERC's annual budget approval process, and will primarily augment the 24x7 nature of the watch.

Section II: E-ISAC Organization Structure, Hours of Operation, and Staffing Levels

E-ISAC Organizational Structure

The E-ISAC is separated into two components: (1) Partnerships and Engagement, and (2) Operations. Partnerships and Engagement consists of cross-sector coordination, member outreach, and policy and coordination. The Operations component is the interface for all information sharing and analysis. Operations consists of three teams: Watch Operations, Cyber Analysis and Context, and Physical Security Analysis.

Watch Operations – All information the E-ISAC receives is routed through the Watch Operations team, which performs initial analysis and then passes the information for detailed action to the respective analysis teams. Watch Operations monitors the operations email account for member and cross-sector sharing, manages the E-ISAC portal, reviews and edits (when necessary, to remove attribution) member postings on the portal, and has primary responsibility for all E-ISAC postings on the portal.

Cyber Analysis and Context – The E-ISAC Cyber Analysis and Context team performs detailed analysis on the cyber security-related information shared by E-ISAC members and partners. The team's goal is to analyze that information to develop and share actionable indicators and the cyber security "big picture" with members and partners. This effort includes vetting information shared by government and cross-sector partners for validity to include the "so what" factor on how certain indicators would apply to a sector. Additionally, the Cyber Analysis and Context team performs analysis of malware samples submitted to the E-ISAC to identify and disseminate indicators that can be used to detect infections or mitigate malware command and control communications.

Physical Security Analysis – The Physical Security Analysis team performs detailed analysis on all physical security events shared with the E-ISAC. When a report is received, the Physical Security Analysis team reviews the information and, as necessary, contacts the relevant entity to seek more detailed information, to determine if there is a bigger threat to the sector. This is especially important in instances of sabotage, vandalism, and explosive devices. The Physical Security Analysis team engages with law enforcement and state fusion centers to help build situational awareness and identify adversary tools, techniques, and procedures that can be shared with industry physical security teams to increase their awareness and protect against similar activity.

E-ISAC Watch Operations Hours of Operation and Staffing Levels

The E-ISAC Watch Operations currently operates with personnel onsite (at 1325 G Street, NW Suite 600, Washington, DC 20005) Monday through Friday from 6 a.m. to 6 p.m. Unless there is an event the necessitates increased after-hours staffing, the only after-hours support to members is provided by a Watch Operations duty officer, rotated through the Watch Operations team on a weekly basis, who monitors the 24-hour incident reporting line. The Watch Operations duty officer is not located onsite outside of normal operating hours.
The E-ISAC Watch Operations is currently staffed as follows:

- One (1) Chief, Watch Operations
- Five (5) Watch Officers:
    1. Watch Manager – Supervisor-level oversight of Watch Officers
    2. Watch Officer: Daily Operations – Watch Floor facility maintenance, tour scheduling, morning situation awareness products, etc.
    3. Watch Officer: Metrics and Reporting (Vacant) – Provides metrics on Watch Operations to NERC and E-ISAC leadership (portal visitors and usage, support ticket tracking, etc.)
    4. Watch Officer: Technical Assessments – Quick-hit, but deeper-dive analysis of cyber event reporting

5. Watch Officer: Open Source Intelligence (Vacant) – Development and production of all analytical products produced by Watch Operations

The E-ISAC's 2019 budget includes the augmentation of existing capabilities with the following additional personnel:

1. Watch Officer: Security Analysis – Specializes in analyzing and information sharing of physical security-specific events
2. Watch Officer: Interagency Liaison – Rotates between the National Cybersecurity and Communications Integration Center (NCCIC) watch floor or other entities with standing information-sharing programs

Section III: Value of Expanding to Include 24x7 Onsite Capabilities

As noted above, the E-ISAC does not operate on a 24x7 basis. As the E-ISAC continue to mature, however, there are benefits to be gained by expanding operations to include certain 24x7 onsite operations. The following is a discussion of the benefits of having 24x7 capabilities.

Increased Capability to Address Events Outside of Normal Hours – To date, there have been only a few events that have occurred outside of normal business hours that required substantive analysis and immediate communication with stakeholders. Such events, however, could become more common as the risk to the nation's critical infrastructure increases.[38] Business hours in many of the nation states that pose the greatest cyber threats to U.S. interests – e.g., Russia, China, Iran, and Democratic People's Republic of Korea[39] – are generally opposite those in North America. Hackers may also target members and partners in North America during reduced staffing periods (e.g. overnight, holidays, and weekends).[40] With an onsite 24x7 staffing presence, the E-ISAC would improve its ability to timely analyze and respond to potential events that occur outside of normal business hours.

Development of Actionable Intelligence for Daytime Staff – As the E-ISAC continues to develop and establish new data sources, 24x7 onsite staffing would allow the E-ISAC additional time to perform analysis to develop and share actionable intelligence with member night shift personnel or to have reports available for daytime staff to assess at the beginning of their work day. Rapid access to information is critical when network defenders are working through the Cyber Kill Chain model to remediate cyber-attacks.[41]

The value of and need for 24x7 onsite capabilities is dependent on increased flow of data into the E-ISAC. Without increased data and additional tools and capabilities to analyze the data, the move towards 24x7 may not provide the intended benefits described above or warrant the additional expenditure of resources. To that end, the E-ISAC is already taking steps to increase data sharing from members and seeking new data sources to which it has access:

- **Member Engagement** – The E-ISAC is currently engaging in a number of efforts to improve the data flow from E-ISAC members. Among other things, the E-ISAC expects increased data flow from: (1) the Industry Augmentation Program; (2) expanding the number of CRISP companies to provide additional insight in the classified threats facing our members' information technology systems,[42] and (3) developing advanced analytics capabilities (e.g., the Cyber Automated Information Sharing System). The E-ISAC is also taking steps to increase membership overall.

[38] Two such events include attacks by the hacker group WannaCry, which was believed to be responsible for network compromises primarily located in Asia, and the Petya/NotPetya ransomware attack that affected computers across Europe.
[39] Based on the *Worldwide Threat Assessment of the US Intelligence Community*
[40] https://www.curotec.com/insights/christmas-hackers-attacks-increase-around-holidays/
[41] Research has been conducted on how the Cyber Kill Chain model can specifically apply to the sector. For one such endeavor, see the SANS Institute report *The Industrial Control System Cyber Kill Chain*
[42] Pacific Northwest National Laboratory, located in Washington State, is a key source of CRISP analysis. Moving to 24x7 operations will expand the opportunities for analysts in Washington, D.C. to communicate with their counterparts at the lab.

- **Government Partnerships** – The E-ISAC is renewing and expanding relationships with federal government partners (e.g., Departments of Energy and Homeland Security, FBI, Canadian Cyber Incident Response Centre) to increase information sharing and data flows, and gaining additional credentialed access where appropriate. These relationships will expand access to government-informed information and analysis.
- **International Partnerships** – The E-ISAC is expanding partnerships with international counterparts. During the June 2017 cyberattacks that began in the Ukraine and spread across Europe, the E-ISAC worked with analysts at the National Cyber Security Centre in the U.K. to assess the tactics, techniques, and procedures being used by the adversary and to provide updated information to members.[43] The E-ISAC is also fostering a relationship with the nascent Japan Electricity Information Sharing and Analysis Center, and the Canadian Cyber Incident Response Center. The information gained from these international engagements will help provide a more complete assessment of, and ability to act on, attacks against international electricity sector partners which could also threaten the North American grid.
- **Strategic Vendor Partnerships** – The E-ISAC is focused on developing strategic relationships with intelligence-reporting providers to provide insight into threats facing the sector's industrial control system technologies.[44]

Section IV: Recommended Level of 24x7 Onsite Capabilities

Given the value that 24x7 operations could provide to its members and partners, the E-ISAC recommends expanding the role of the Watch Operations team to include certain 24x7 onsite capabilities. Depending on the level of data flow into the E-ISAC, the goal is to have always have one-to-two E-ISAC Watch Officers onsite outside normal business hours.

The responsibilities of the Watch Officers onsite after normal business hours would shift slightly from the duties traditionally conducted by Watch Officers during normal business hours (i.e., monitor and respond to incoming information and perform a "quick hit" initial analysis of incoming data). For Watch Officers that staff the night, weekend and holiday hours, the nature of their responsibilities shift more towards analysis. Baring a substantial security event, after-hours communication and data flow from members and partners—including international partners—is not expected to be as extensive as that received during normal business hours. As such, while a primary focus would continue to be monitoring data feeds and responding to member and partner inquiries, the after-hours onsite Watch Officer would focus more on analysis of data and the development of actionable intelligence reports for daytime staff.

Section V: Staffing Requirements for Expanded Operations

The E-ISAC recommends that expansion to 24x7 capabilities to the level discussed in the previous section be accomplished in stages through 2020 and beyond. Using a phased approach will allow the expansion to move in parallel with the E-ISAC's plans to increase data flow and deploy additional analytical tools and capabilities. As noted, the value of expanding operations to include 24x7 capabilities depends, in large part, on increasing the data flow in order to warrant the additional resources. A phased approach would provide the ability to reassess the timing of additional projected resource needs on an annual basis during NERC's budget approval process. The E-ISAC recommends that the expansion proceed as outlined below.

[43] E-ISAC portal posting *Update 2 - Continuing Cyber Attacks Affecting U.S., Overseas Entities*

[44] Pilots are currently being negotiated with Dragos and N-Dimension.

Table 1: Watch Officer Assignments and Coverage				
Year	**Monday–Friday 6:00 a.m.–6:00 p.m.**	**Monday–Friday 2:30–11:00 p.m.**	**Monday–Friday 10:00 p.m.–6:30 a.m.**	**Weekends/Holidays 12:00 a.m.–12:00 p.m.**
2018	Maintain current planned staffing levels	N/A	N/A	N/A
2019	Add two watch officers from 2018 levels	Add one watch officer	Add one watch officer	N/A
2020	Add one watch officer from 2019 levels	Maintain staffing level from 2019	Maintain staffing level from 2019	Add two watch officers
2021	Add one watch officer from 2020 levels	Add one watch officer from 2020 levels	Add one watch officer from 2020 levels	Maintain staffing level from 2020

The table below provides the recommended phase-in plan for additional personnel required to meet the expanded operations for each of the next three years.

Table 2: Watch Officer Totals and Cost					
Year	**Increased Watch Personnel for Regular Hours (2018 Long-Term Strategy)**	**Proposed Additional Watch Personnel for 24x7 Coverage (Incremental to 2018 Long-Term Strategy)**	**Total Proposed Watch Staffing, including 24x7 Watch Capabilities**	**Estimated Incremental Cost (including salary, incentive, benefits) (24x7 Watch Capabilities)**	**Running Total for Estimated Incremental Cost (24x7 Watch Capabilities)**
2018	1	0	6	N/A	-
2019	2	2	10	$370,000	$370,000
2020	1	2	13	$370,000	$740,000
2021	1	2	16	$370,000	$1,110,000

As noted above, this proposed plan and resources needs for future years (2020 and beyond) will be subject to review and approval in the context of NERC's annual budget approval process.

Exhibit F – CMEP Technology Project Business Case

Executive Summary

With the ERO Enterprise at a critical point in its maturation, the Compliance Monitoring and Enforcement Program (CMEP) Technology Project is a strategic opportunity to significantly improve the productivity and effectiveness of the ERO Enterprise, and will provide benefits to all those impacted by our work: registered entities, Regional Entities, and NERC. This enterprise-level program will support the following objectives:

- Protect and maintain the reputation of the ERO as a credible regulator through consistent and objective implementation of generally accepted professional standards and best practices, as well as requirements established through the Rules of Procedure (ROP)
- Ensure consistency in practices and data gathering by aligning common CMEP business processes across the ERO Enterprise
- Increase productivity of compliance work activities for registered entities as well as across the ERO Enterprise through easier data entry and access to information, as well as through the use of workflows and collaboration tools
- Enhance the effectiveness of the ERO Enterprise by increasing its ability to share and analyze reliability risk and compliance information across NERC and the Regional Entities
- Reduce total combined NERC and Regional Entity IT capital investments and maintenance costs for CMEP-related applications. Current annual licensing and maintenance fees across the ERO Enterprise are $1.1M

Once implemented, the new solution will give NERC and the Regional Entities a greater level of visibility into identifying and managing reliability risk. The ability to catalogue and manage reliability risks across North America will combine with the ability to see those risks within the context of compliance trends, performance analysis, and forward-looking assessments. Together, these elements will provide deep and broad views of reliability across the ERO Enterprise, leading to new insights into data-informed reliability risk management. Such visibility is essential to the continuing maturation of the ERO Enterprise and the achievement of our reliability mission.

Table 1 - Program Information at a Glance

Program Name	CMEP Technology Project
Portfolio	ERO Enterprise
Executive Sponsors	• Jim Robb, President and CEO, NERC • Jim Albright, Vice President and COO, MRO
Project Sponsors	• Stan Hoptroff, Vice President and CTO, and Director of Information Technology, NERC • Ken McIntyre, Vice President and Director of Standards and Compliance, NERC • Sonia Mendonça, Vice President, Deputy General Counsel and Director of Enforcement, NERC
Program Areas	Compliance and Enforcement
Project Type	New Functionality
Total Estimated Capital Investment	$5.1 – 5.5M, completing in 2020
Estimated Annual Operating Costs	$780k per year over five years (2018-2022)
Estimated Return on Investment	$1.47M in 2021 (year 5), based on medium cost and medium benefit estimates used in cost/benefit analysis
Stakeholders	NERC, Regional Entities, and registered entities
Proposed Timeline	2017-2020

Strategic Opportunity

The CMEP Technology Project is a culmination of strategic efforts that began in 2014 with the goal of improving and standardizing processes across the ERO Enterprise. As the ERO Enterprise matures to use a risk-based approach in its regulatory posture for the CMEP, the need to develop a more comprehensive system to manage and analyze information is more acute. The ERO Enterprise has great discretion in the development of its regulatory oversight and enforcement – and it is essential that we show that discretion is exercised with due care and in a competent manner. Without a robust, comprehensive system, verifying the effectiveness of ERO Enterprise oversight of the almost 1,500 registered entities becomes more difficult with the reliance on a patchwork of tools and information spread across the eight Regions and NERC. Regional and NERC senior management require a mechanism to provide assurance that these risks are managed through a comprehensive system benchmarked around well understood processes designed to prevent regulatory failures.

While a number of past efforts focused on improving the effectiveness of various processes used in compliance monitoring and enforcement, the tools used in the execution of those processes largely rely on the technology skills of compliance and enforcement staff. Other than the enforcement processing systems (webCDMS, CITS and CRATS)[45], a number of manual processes are used in place of a single, enterprise-class system. As a result, much of the CMEP staff spends time creating, updating, and maintaining these manual processes. The result is less time available for the central mission of reliability risk management and control.

At the same time, registered entities face a regulatory environment in which the information they provide and the way performance is measured can change depending on the location of the assets they own or operate. The organic growth of regional tools and best practices across North America led to small differences in implementation that, while achieving the same goals, create additional cost and complexity in terms of complying with the Reliability Standards. Lacking a common foundation upon which to judge compliance, auditor expectations in different Regions can be inconsistent. In some cases, evidence judged as sufficient in one Region may be seen as questionable or insufficient in another.

The reliability goals of the ERO Enterprise drive the execution of the CMEP. Roughly 39 percent of the resources across the ERO Enterprise are focused on Compliance and related enforcement activities, making it the highest area of resource allocation. Given the high allocation to these responsibilities, the need to seek opportunities for ways to improve the productivity and effectiveness of the ERO Enterprise is clear.

ERO Enterprise Resource Allocation to Strategic Goal Areas

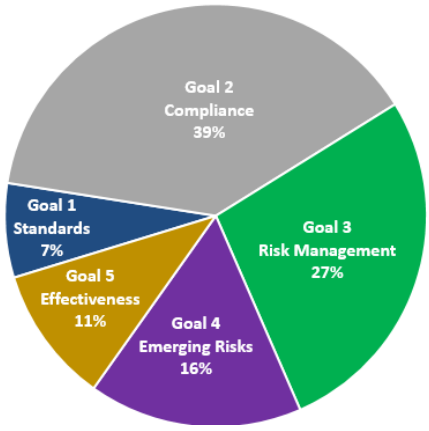


Figure 1

The NERC Information Technology team, working with thought leaders from both NERC and the Regional Entities, developed a vision and roadmap to move away from the mix of approaches and toward a single, common system to support ERO Enterprise needs and increase consistency across the ERO. During the past two years, the ERO Enterprise investigated, validated, and refined this approach. As a result, the ERO Enterprise seeks to identify and implement a common, best-in-class system that

[45] The OATI Web Compliance Data Management System (webCDMS), the Guidance Compliance Information Tracking System (CITS), and the Guidance Compliance Reporting and Tracking System (CRATS).

aligns with audit and risk-management industry best practices. Such alignment will help ensure the operational success of the ERO, while moving the ERO Enterprise to a technology that is routinely enhanced and updated based on audit industry improvements and lessons learned.

Recognizing the magnitude of this endeavor, a governance group comprised of leaders from both NERC and the Regional Entities was assembled to select a consulting partner to help guide the ERO Enterprise through this next phase in its maturation. Through a robust evaluation process, the team chose Deloitte Consulting to serve as this guide. Identified as a visionary leader in Risk Management Consulting Services, based on both its ability to execute and the completeness of its vision in the Gartner Magic Quadrant[46] report, Deloitte was retained by NERC to drive the adoption of common business process and practice in the CMEP, and to assist in identifying a tool that will best serve the needs of the ERO Enterprise. Deloitte will also assist in driving the overall implementation effort.

Figure 2 - Gartner Magic Quadrant for Risk Management Consulting

Through this solution, operational information will be available across the ERO Enterprise as CMEP activities unfold. This will eliminate the delays and complexity associated with exchanging information between systems as we do today, as well as reducing the manual work that goes into collecting and exchanging non-standard data both among Regional Entities and between Regional Entities and NERC. Moving to a common solution will enable both NERC and the Regional Entities to do more detailed reporting on risk trends and operational analysis, further increasing productivity and effectiveness, and provide new ways to undertake research and analysis of compliance performance and reliability risks.

Beyond information analysis, alignment of the chosen solution with audit industry best practices and tools will provide additional benefits. Annual planning, entity-specific audit planning, and actual compliance monitoring will be facilitated by a system designed and purpose-built to support these processes, leading to increased productivity and effectiveness.

Stakeholder Involvement

In addition to the benefits for the ERO Enterprise, moving to a common tool also benefits registered entities. When implementation is complete, the new system will provide a standardized interface through which registered entities can interact with the ERO Enterprise. This will help ensure consistency of processes, templates, and communications during the implementation of the CMEP, reducing both the perception of inconsistent treatment and the corporate risk associated with those perceptions.

[46] From Magic Quadrant for Risk Management Consulting Services, Worldwide, 5 November 2015. *This graphic was published by Gartner, Inc., as part of a larger research document and should be evaluated in the context of the entire document. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

Additionally, registered entities will also be able to use data and information from the new system to help evaluate and manage their own reliability risk. This will build on the existing feedback mechanisms and provide greater functionality in this area than that which exists today.

The project team will solicit stakeholder input through a series of communications and outreach through the various stakeholder groups, including the Compliance and Certification Committee (CCC), the Member Representatives Committee (MRC), and other relevant committees and subcommittees, as appropriate. Specifically, the project team will solicit feedback regarding current legacy system challenges and opportunities that this initiative should address.

The reputation and credibility of the ERO Enterprise relies on the ability to demonstrate that authority and discretion are used in the public interests to maintain the reliability and security of the bulk power system. The remaining sections of this business case provide additional detail and further explain the rationale for moving forward with this endeavor.

Business Opportunity Assessment and Analysis

Current State

Since 2007, the Regional Entities and NERC developed their own processes and systems to support the mission of the ERO Enterprise consistent with the CMEP and the ROP. During the early stages of the ERO Enterprise (NERC and the Regions), broad flexibility was needed to meet the statutory start-up date of the ERO. But this swift implementation strategy came with a cost – varying business processes with varying tools (e.g., CRATS, CITS, and webCDMS), creating both perceived and real consistency issues in the implementation of the CMEP. It also resulted in the inability to share information across the ERO Enterprise, and difficulty in documenting conformance with applicable professional standards and the ROP.

During the past 10 years, the Regional Entities and NERC matured, as have CMEP business processes and tools. At this stage of the ERO Enterprise development, it is prudent and necessary to evaluate and develop better-aligned business processes and tools by leveraging and blending the collective experiences of the Regional Entities and NERC. In addition, given the growth in compliance requirements across many industries, more commercial application options are available today as compared to just a few years ago.

The lack of a common technology platform contributes to inconsistent use of data labels and terminology, resulting in inefficiencies to reconcile data from disparate systems to accurately analyze reliability and compliance data and trends. This inconsistency is illustrated below by showing:

- Only limited interaction between the NERC framework and the Regional processes – specifically, at the interface between the CRATS system and the CITS and webCDMS systems (illustrated by the green "Region-Defined Tools and Processes" and the blue "NERC-Defined Tools and Processes")
- A smaller set of "rigid core" data used at the Regions consistent with the NERC use, limited to noncompliance and mitigation data (Illustrated by the blue "NERC Rigid Core Data")
- Multiple processes or approaches to CMEP work, which results in real and perceived inconsistencies (illustrated by both the green "Regional Flexible Edge Data" and the green "Region-Defined Tools and Processes")

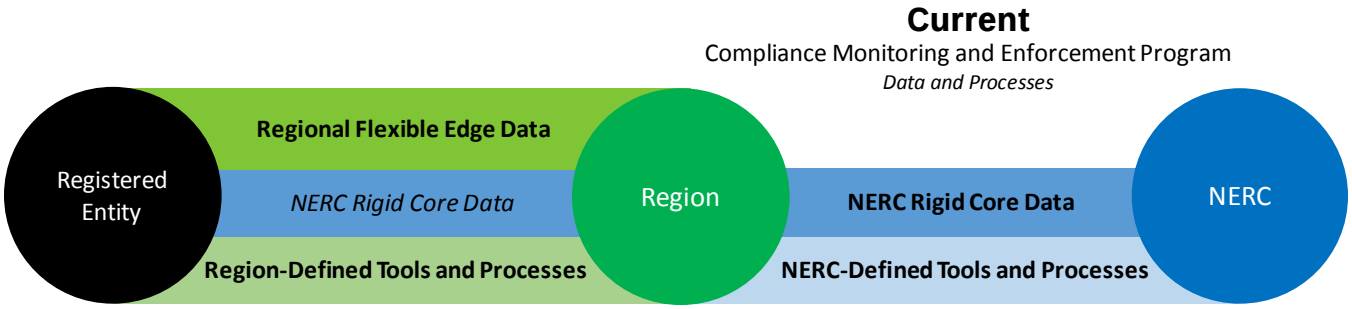


Figure 3

Future State

In the proposed future state, the ERO Enterprise data and processes model is expanded to include more of the Regional processes (moving some of the green "Region-Defined Tools and Processes" and "Regional Flexible Edge Data" into the blue "Rigid Core"). In so doing, common processes, procedures and terminology can be adopted to better drive alignment and reduce real and perceived inconsistencies, while reducing costs across the ERO Enterprise. The future state proposes replacing the current CMEP tools from OATI and Guidance with one system used by NERC and the Regions. The cost for that replacement is included in the budget estimates.

To address Region-specific needs, it is expected that Regional Entities may need to continue to collect Region-specific data and/or use Region-defined tools and processes for unique analyses (represented by the remaining green areas). The future model allows for this flexibility (subject to ERO oversight), with an expectation that the general preference will be to use rigid core data, as well as ERO Enterprise defined tools and processes, where possible.

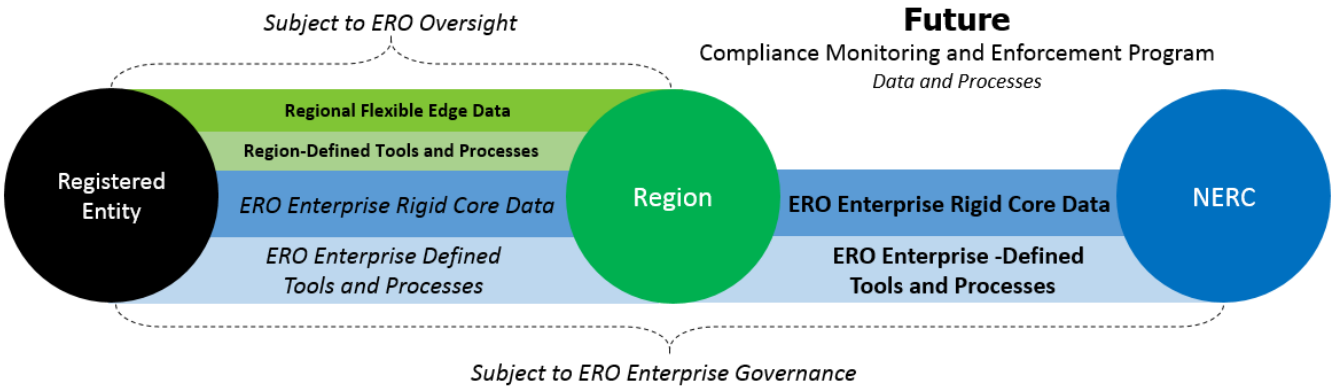


Figure 4

The solution approach shown below illustrates several interrelated functional components that will comprise the proposed ERO Enterprise CMEP system. The following diagram and discussion reviews the relationship between those components.

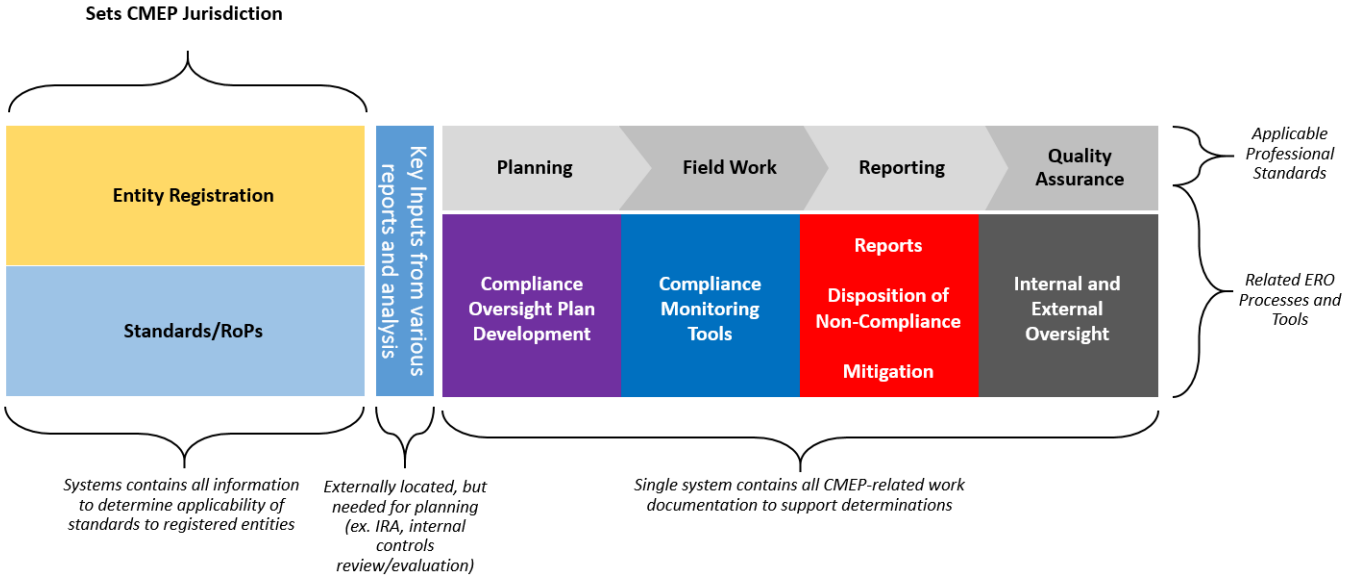


Figure 5

CMEP jurisdiction is established through an entity registration database, standards database, and the applicable ROP rules and any exceptions (i.e., exclusions from jurisdiction resulting from BES process). The jurisdiction elements form the foundation for the CMEP work and serve as the starting point for compliance oversight plan development, a key part of the proposed system. As illustrated, the overarching workflow matches normal practices found in authoritative assurance standards (e.g., the Government Accountability Office's Generally Accepted Government Auditing Standards, or GAGAS, also known as the "Yellow Book"): planning, field work, reporting, and quality assurance.

Compliance oversight planning is a comprehensive endeavor and requires linkages from various reports and analysis, including inherent risk assessments, past compliance history, miscellaneous technical reports, periodic reporting of key information, events and other information. At this time, much of the information will serve as inputs into the compliance oversight plan development; but, if this information can be directly accessed through the proposed CMEP system, the specifications will be noted as such.

After the compliance oversight plan is developed (which includes the scope of the Standards and Requirements for monitoring and the monitoring tools themselves, e.g., audits, spot checks, self-certifications), the associated notifications, data request forms, etc., can be generated. In some instances, registered entities will require access to the system to submit completed data requests (e.g., "evidence"), self-certifications, etc. In addition, registered entities self-report, a key compliance monitoring activity. Self-reporting will also be included in this part of the system and will require registered entity access. While investigations are less frequent, this part of the system will also be used for documenting the planning and field work associated with investigations.

Reporting aspects of the proposed system will accommodate audit, spot reports, and dispositions of non-compliance (e.g., compliance exceptions, notices of penalty, settlements). In addition, there will be a separate mitigation process in the system to document and track mitigation of all non-compliance; this will require access by registered entities.

Lastly, the system will address oversight through quality assurance mechanisms. Quality assurance is both a Regional and NERC responsibility. Within this part of the system, both NERC and the Regions will have the ability to document their oversight activities on the CMEP work performed. The system should be designed in such a fashion that NERC can access internal Regional oversight activities to determine its level of external oversight. Quality assurance should be accessed only by NERC and the Regions.

Throughout the system development, careful consideration will be given to ensuring appropriate access controls and protections are in place to comply with rules around confidentiality of information and security of sensitive, critical infrastructure information.

Business Value Analysis

NERC's standard business value analysis process will be used to identify expected benefits and beneficiaries, and how those benefits will manifest and be measured to ensure overall project success. NERC evaluates six distinct benefit areas as shown in the table below. In each area, an expected benefit is proposed, as well as how that benefit could be measured.

Table 2 – Benefits and Measurements

Benefit Area	Benefit Summary	Measurement Approach
Reduce Reliability Risk	Improved visibility will enable the ERO Enterprise, registered entities, and industry, in general, to target emerging reliability risks more quickly.	Feature Delivery Confirmation
	Increased transparency will assist NERC in validating that reliability risks are managed and addressed in the compliance monitoring process (understanding what requirements were audited and complied with, as opposed to only seeing violations found and reported during the enforcement process. Help show how monitoring process choices relate back to the registered entity risk assessment).	Feature Delivery Confirmation

Table 2 – Benefits and Measurements		
Benefit Area	Benefit Summary	Measurement Approach
Increase Capability	Ability to view an aggregate risk profile for a given Region, as well as look for trends and extent of condition across Regions.	Feature Delivery Confirmation
	Ability to view a risk profile that shows compliance history trends in various areas for each registered entity, as well as look for trends across registered entities.	Feature Delivery Confirmation
	Ability to view compliance history trends by standard or standard family.	Feature Delivery Confirmation
	Increased analytics and reporting capability.	Feature Delivery Confirmation
	Registered entities have a single system for managing and submitting supporting documentation.	Feature Delivery Confirmation
	Capability to share information between and among NERC and Regions within the tool.	Feature Delivery Confirmation
Reduce Corporate Risk	Consistent application of CMEP and ROP across the ERO Enterprise including fair and objective outcomes.	ERO Internal Audit Results
	Reduce new significant noncompliance findings in NERC's implementation of the Regional Entity oversight plans or adherence to the ROP with regard to Compliance Monitoring and Enforcement.	ERO Internal Audit Results
Increase Work Quality	NERC and Regions report perceived increased quality in data and work products.	Annual Survey
	Registered entities report perceived increased quality and consistency in data and work products.	Annual Survey
	Registered entities report increased consistency in interactions with the Regions with regard to the CMEP.	Annual Survey
	Elimination of manual data exchange steps between modules (from planning to monitoring to enforcement, and from the registered entities to the Regions to NERC), reducing transcription errors.	Feature Delivery Confirmation
	Standardized data definitions within a single system will reduce errors.	Feature Delivery Confirmation
Increase Productivity	When asked, registered entities report increased productivity in their interactions with the CMEP process.	Annual Survey
	Reduced processing time of various steps with the CMEP.	($) Specific Metric (compared to historical averages)
	Increased automation of routine CMEP activities.	($) Feature Delivery confirmation (specific activities to be determined in the future).
	Regions and NERC will see reduced manual CMEP labor (implying resources are focused instead on risk-based CMEP analyses and activities).	($) Time Tracking: Total number of hours of manual CMEP Labor reported by ERO Enterprise staff

Table 2 – Benefits and Measurements		
Benefit Area	Benefit Summary	Measurement Approach
		will trend down from 2018 to 2022
	Regional risk, IRA, entity history and other supporting analyses used to create compliance oversight plans are easily accessible and analyzed.	($) Feature Delivery Confirmation
Reduce Cost	Reduction or elimination of costs associated with webCMDS, CITS, and CRATS before the end of 2021.	($) Year to year cost comparison.
	See financial analysis for more details.	

Financial Analysis

The CMEP Technology Project will be implemented in phases. As each phase is launched, the detailed scope, budget, and resources for those phases will be defined and approved through the program governance structure.

The financial analysis below is based on NERC's initial research, begun in late 2014 with Gartner, Inc., a recognized leader in information technology research and advisory services. As a Gartner client, NERC IT solicited their expertise and research capability for possible solutions. The recommendation was to evaluate a series of tools in the Governance, Compliance, and Risk (GRC) platform arena.

NERC conducted an initial Request for Information (RFI) within the GRC vendor community. The investment numbers below are based on the average costs from the responses. The next steps are to conduct a formal Request for Proposal beginning Q3 2017 with detailed business requirements in hand, and use a rigorous selection process to choose the platform and vendor best suited for ERO Enterprise. An updated capital and cost benefit analysis will be conducted after the RFP results and recommended vendor selection are known.

Estimated Capital Investment

Table 3

	2017	2018	2019	2020
TOTAL CAPITAL COST BY YEAR	$280,000	$1,548,000	$1,768,000	$1,507,000
TOTAL CAPITAL INVESTMENT	$5,103,000			

Estimated Annual Operating Costs

Table 4

	2017	2018	2019	2020
TOTAL ANNUAL OPERATING COSTS	$0	$747,000	$735,000	$805,000

Estimated Return on Investment (ROI)

NERC's standard ROI model was used to estimate financial benefits with the following assumptions:

- Estimated costs are considered at 90 percent of base estimate, 100 percent of base estimate, and 130 percent of base estimate.
- Estimated benefits are considered at 50 percent of base estimate, 100 percent of base estimate, and 150 percent of base estimate.
- Fees paid for CITS, webCDMS, and CRATS will no longer be paid starting in 2021.
- Staff at NERC and the Regions in the following programs are estimated to see increased productivity from the implementation of the new tool as follows:

	Expected Increases in Productivity				
	Impacted FTEs	2019	2020	2021	2022 and Beyond
Core Regional CMEP Staff	176	4.50%	8.25%	12.00%	15.00%
Core NERC Enforcement Staff	8	3.38%	6.19%	9.00%	11.25%
Core NERC Regional Entity Assurance and Oversight staff	5	3.38%	6.19%	9.00%	11.25%
Core NERC Compliance Analysis, Registration, and Certification staff	3	2.25%	4.13%	6.00%	7.50%
Remaining CMEP Staff	93.95	0.23%	0.41%	0.60%	0.75%
Core RAPA, RASA, EA, PA Staff	51	0.68%	1.24%	1.80%	2.25%
Remaining RAPA, RASA, EA, PA staff	65.1	0.23%	0.41%	0.60%	0.75%
NERC Standards Information Staff	4	0.68%	1.24%	1.80%	2.25%
Remaining Standards Staff	24.85	0.23%	0.41%	0.60%	0.75%
TOTAL Impacted ERO Enterprise Staff	430.9	2.10%	3.85%	5.60%	7.00%
	Average Productivity Increase				
		Implementation of Compliance Oversight Plan Development Module and Monitoring Tools	Implementation of Enforcement Module provides benefit, but learning curve hinders full benefit	As users gain experience and become familiar with the tool, benefits increase	Ongoing experience leads to full benefit realization

Table 5 – Productivity Benefits -

ROI is positive in five of the nine considered scenarios over five years, with the all scenarios positive in ten years. Mean break-even year is roughly 2021 (after full functionality is delivered). A net reduction in annual CMEP tool-related expenditures begins in 2021.

Figure 6 on the following page illustrates the estimated annual cumulative costs and hard dollars saved based on the data shown in Tables 3 and 4, and estimated annual cumulative benefits in soft dollars to represent efficiencies gained as described in Table 5 above. The points where the lines intersect represent the estimated break-even points for the nine scenarios considered. This same information is shown in Table 9. Tables 6 through 8 show the 3-year, 5-year, and 10-year estimated returns on investment based on this same data, assuming 2.5 percent annual increase in payroll expenses and a 5 percent discount rate.

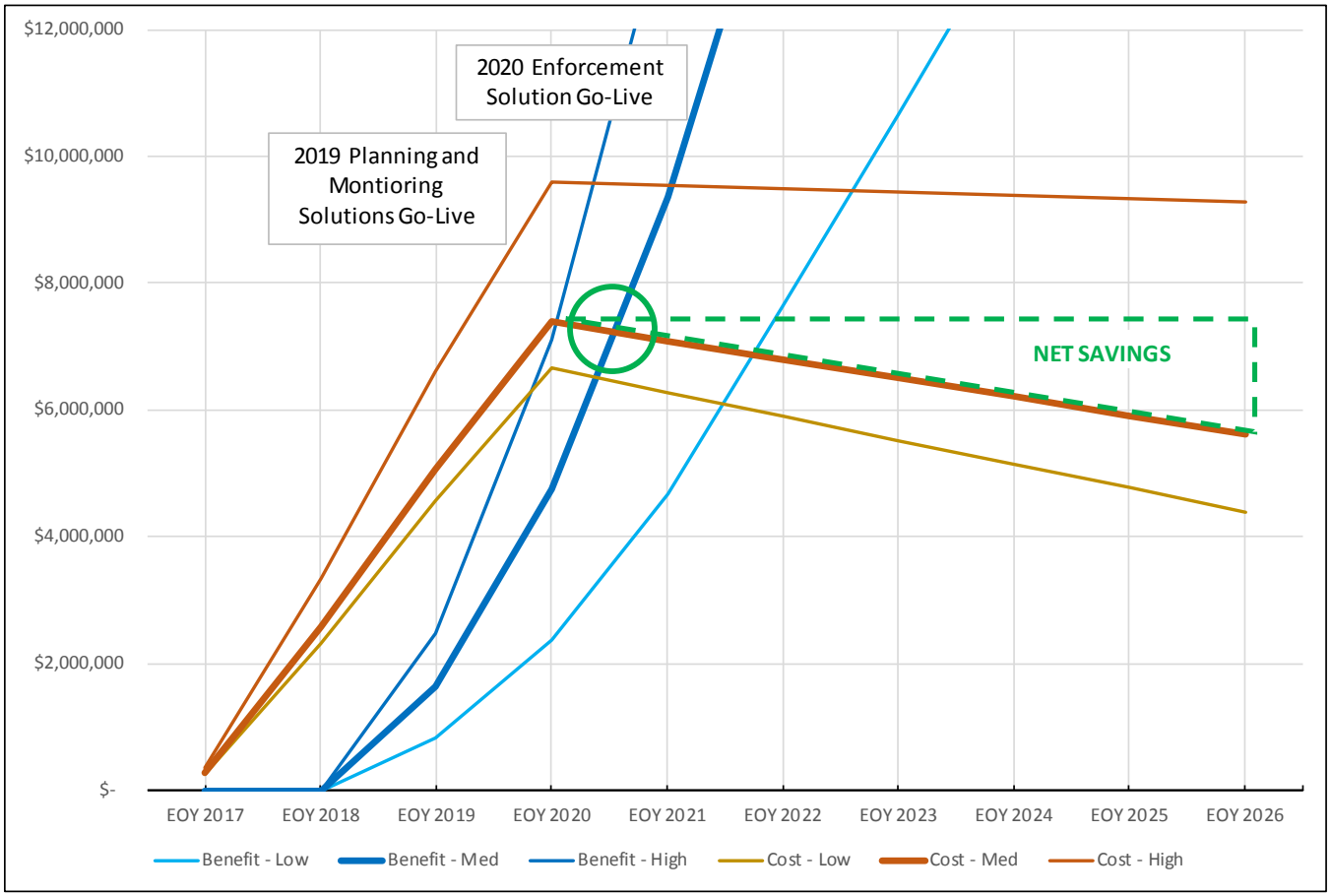


Figure 6 – Costs and Benefits Estimates Plots

3 Year PV	Benefit		
	Low	Medium	High
Low Cost	-$3,515,293	-$2,768,715	-$2,022,136
Medium Cost	-$3,988,835	-$3,242,256	-$2,495,677
High Cost	-$5,409,459	-$4,662,880	-$3,916,301

5 Year PV	Benefit		
	Low	Medium	High
Low Cost	-$1,770,302	$2,209,617	$6,189,536
Medium Cost	-$2,509,755	$1,470,164	$5,450,084
High Cost	-$4,728,113	-$748,193	$3,231,726

10 Year PV	Benefit		
	Low	Medium	High
Low Cost	$10,601,992	$25,617,112	$40,632,233
Medium Cost	$9,575,892	$24,591,013	$39,606,133
High Cost	$6,497,593	$21,512,714	$36,527,834

Break Even Year	Benefit		
	Low	Medium	High
Low Cost	2022	2021	2020
Medium Cost	2022	2021	2021
High Cost	2023	2022	2021

Tables 6 through 9 – ROI Scenarios and Break Even Year

As part of the benefits measurement process, many of the assumptions used within this analysis will be validated. See Table 2 for specific measurements, identified with a "$."

Cost Capitalization – Accounting Treatment

The costs shown above only reflect the external expenses related to the project (e.g., consultants, hardware and software). Any project undertaken by NERC's project management and information technology team also uses internal resources during various phases of the project, including requirements gathering, system development, and project management. However, as a normal practice, NERC does not include these internal labor costs in the business case analysis of projects. NERC does not currently anticipate any additional internal staffing needs to support the success of this project and plans to prioritize current internal resources appropriately.

While the internal labor costs are not included from an analysis and business case perspective, some of those costs will be capitalized as a part of the project cost according to prevailing accounting rules. In other words, the external costs ultimately spent on this project will be different than the costs reflected for accounting purposes over time, the latter being higher because of the capitalization of certain internal labor costs. This is common for projects that are primarily developed by external resources.

CMEP Technology Project Governance

The CMEP Technology Project governance model is comprised of executive oversight, technical leadership, and program execution from both NERC and the Regions. The governance model includes the following groups and participants:

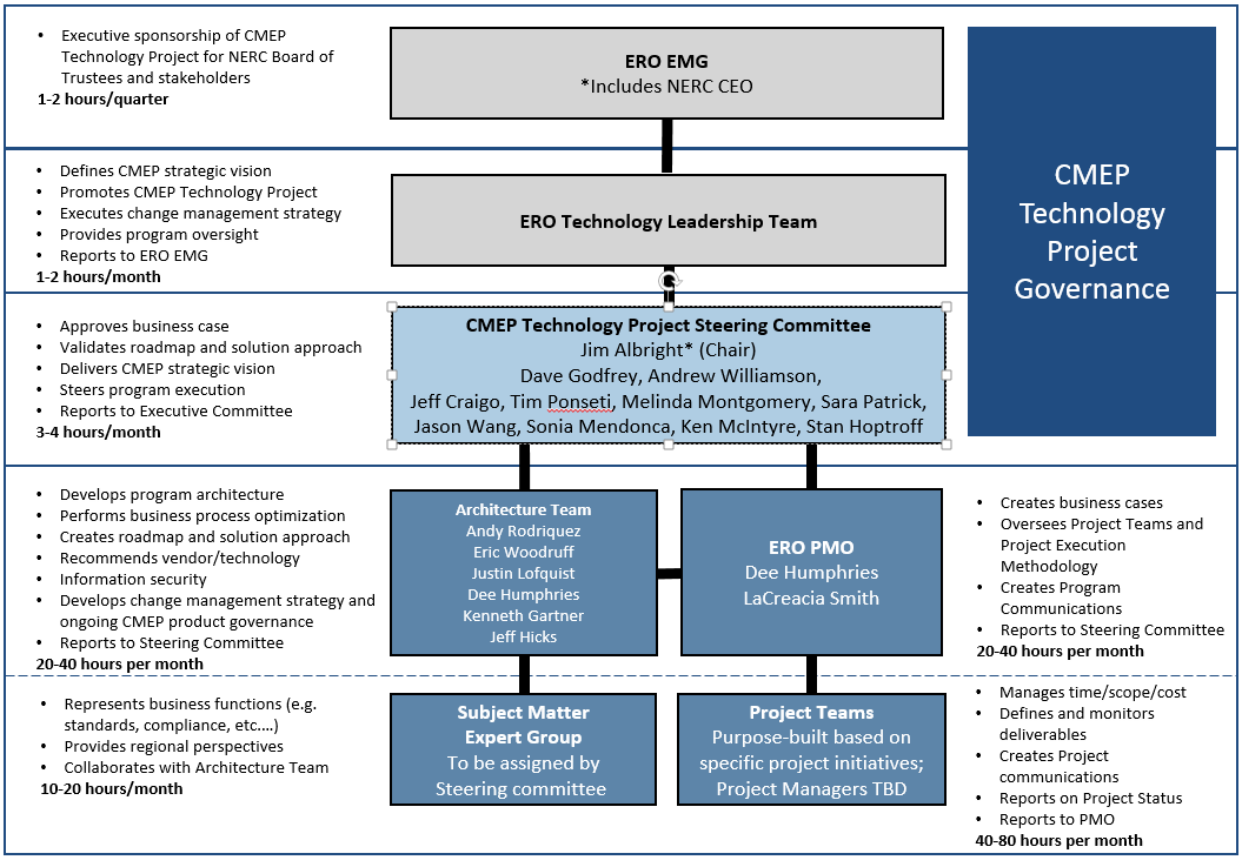


Figure 7 – Project Governance

The above groups will be responsible for overseeing program and project execution. To ensure long-term viability, business process and product governance should continue as the CMEP Technology Project evolves. The following diagram illustrates the proposed transformation from project to product governance.

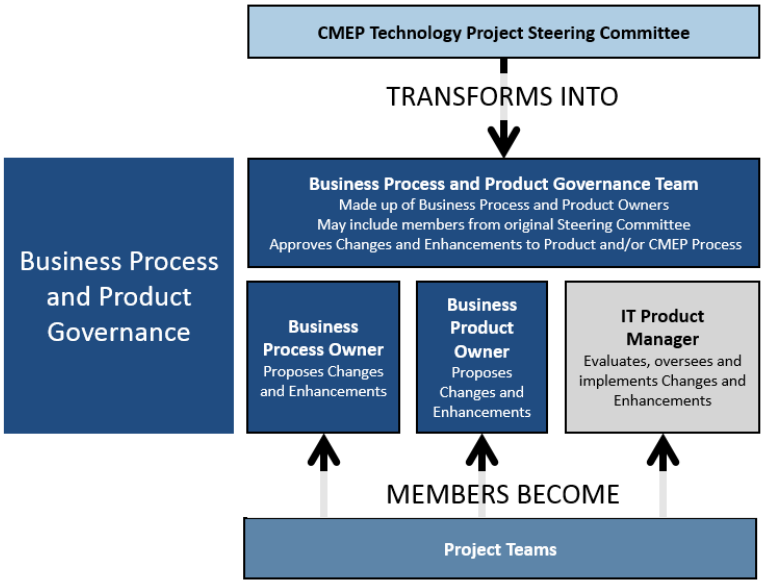


Figure 8 – Ongoing Governance

CMEP Technology Project Execution

The ERO Project Management Office will oversee the execution of each project and the overall program, following standard procedures and best practices as defined by the Project Management Institute's *Project Management Body of Knowledge.*

The PMO will provide project management standards in the following areas:

- Risk and issues management
- Scope management
- Human resource management
- Contract management
- Schedule management
- Communications management
- Change control management

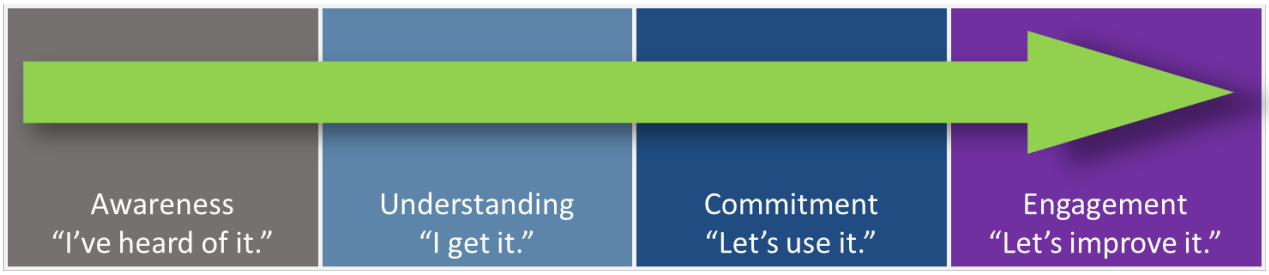
The PMO also provides a rigorous tollgate approach to all initiatives. The tollgate schedule provides accountability in each phase of the project with all deliverables, time management, and budget oversight. At any point in the process, the executive sponsors decide if the project should continue. In addition, the PMO will provide NERC Finance with a monthly overview of the project budget.

PMO Project Tollgate Schedule										
Tollgate		Tollgate 0		Tollgate 1		Tollgate 2		Tollgate 3- END-USER GO-LIVE	Tollgate 4	
Phase	**Initiate**		**Plan/Analyze/Design**		**Develop/Test**		**Deploy**		**Warranty and Support**	**Close**
Purpose	Business justification for project Completion of business case and investment estimate approvals		Entrance Criteria: Approved Business Case and Inclusion on PMO Roadmap Establish scope and resources assigned High-level requirements and vendor selection Architectural solution defined and designed Business and technical processes are designed Scope frozen for identified release		Systems are created and tested		Systems turned over to business for commercial use Organizational changes implemented Users are trained		Post-Go Live warranty and support activities Transition to steady-state operations	Formal project close down Resources released. Contracts closed. Final financials and reporting.

Figure 9 – PMO Tollgates

CMEP Technology Project Communications and Organizational Change Management

A comprehensive change management plan will be developed and executed to facilitate adoption of the program and the business changes that will come with it.



Adoption Stages

Figure 10

The ERO Project Management Office recognizes a four-stage model of organizational change management and user adoption:

- **Awareness.** Stakeholders understand that change is coming, but lack the details or impact to their role.
- **Understanding.** Stakeholders know why the change is happening, when it will affect them, and where it will take place.
- **Commitment.** Everyone knows how the change will affect them and has adopted the change.
- **Engagement.** Everyone is operating in the new environment and actively working to continuously improve the product.

Working with the various governance teams and the NERC communications team, the ERO Project Management Office will craft program and project communication strategies to ensure movement though these four stages is optimal.

CMEP Technology Project Timeline

The timeline for the stages in the CMEP Technology Project will be governed by sponsorship priority, budget, and available resources. Specific dates will be governed by the ERO PMO and announced in subsequent charters.

Overall, the program approach will use the following phases:

- **2017:** Discovery → Plan → Analyze (Requirements) → RFP/Tool Selection
- **2018-2020:** Design → Develop and Test → Incremental Delivery
- **Future:** BES and Facility data integration

The following conceptual planning roadmap illustrates the potential phases of the project. However, until a product is chosen and a more detailed planning effort is undertaken based on that technology, this schedule is conceptual only and will need to be refined as more is learned.

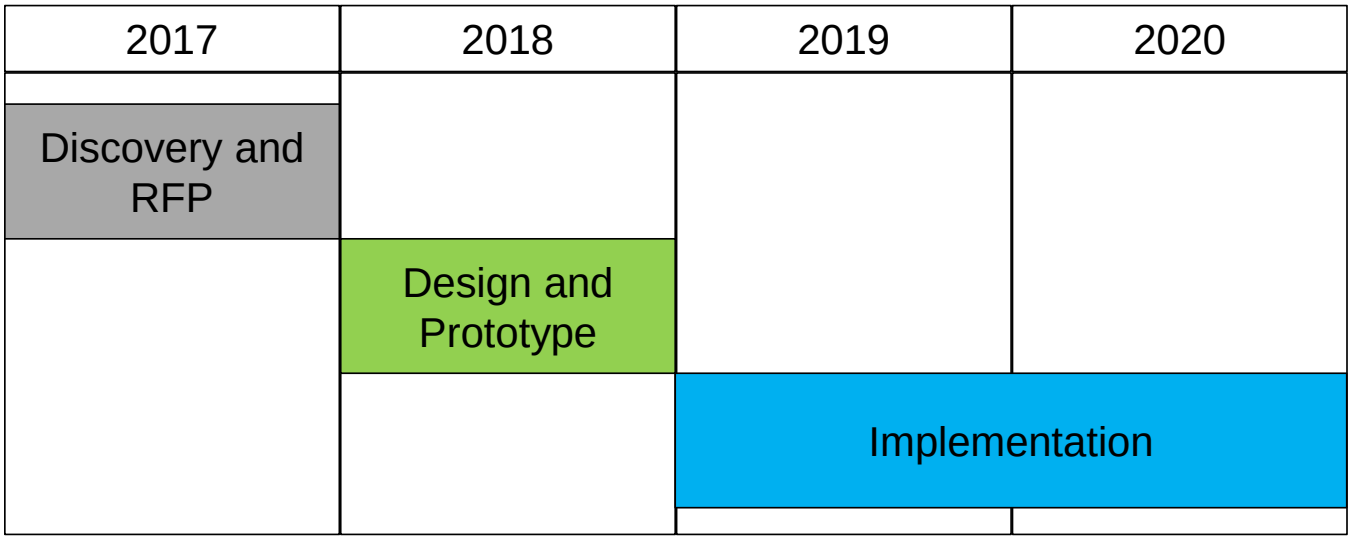


Figure 11

CMEP Technology Project Background

The CMEP Technology Project is one of four strategic vision and technology programs within the broader ERO Enterprise Systems Initiative. The scope of the CMEP Technology Project includes efforts to support a common ERO Enterprise-level CMEP system built from aligned business processes and integrated data sharing. As specific phases are launched, the detailed scope, budget, and resources for those phases will be defined and approved in subsequent charters.

NERC'S initial research began in late 2014 with Gartner, Inc., a recognized leader in information technology research and advisory services. As a Gartner client, NERC IT solicited their expertise and research capability for possible solutions. The recommendation was to evaluate a series of tools in the GRC platform arena. As platforms, they provided integrated sets of services that work together to meet business needs in these areas, rather than piecemeal solutions.

In reviewing this research, NERC discovered these platforms can potentially eliminate much of the manual work conducted across the ERO when executing the CMEP process. NERC then created a strategic roadmap to show how such a tool might be implemented at NERC and the Regions, and the potential benefits.

As part of the initial RFI mentioned earlier, an initial list of nine potential vendors was created, some from Gartner research, others from industry recommendations. Six of these vendors were identified on the Gartner Magic Quadrant. The RFI was issued on September 25, 2015, with responses received November 13, 2015. The vendors/platforms invited to respond the RFI were:

- Certrec
- CMO Compliance
- Cooper Compliance
- EMC/RSA and the Archer platform
- MetricStream and their platform
- Morgan Kai
- Nasdaq and the B-Wise platform
- Resolver
- Thomson Reuters

Seven vendors responded; both CMO Compliance and Thomson Reuters elected not to respond. Upon receipt, NERC staff evaluated the responses based on vendor characteristics, solution features, and technology architecture. The four vendors identified for further consideration were EMC/RSA, MetricStream, NASDAQ, and Resolver. NERC asked these four vendors to set up demonstrations in the second quarter of 2016 for NERC and Regional Staff. Demonstrations were held in June for EMC/RSA Archer, MetricStream, and Nasdaq BWise. Resolver elected not to participate.

A brief introduction to GRC platforms was made with one of the vendors, MetricStream, and an initial demonstration was conducted in February of 2015. This provided clearer understanding of how a GRC system might work for the ERO Enterprise.

Following this, a detailed review of the RFI and its results was undertaken with Gartner on October 24, 2016, and then two sessions with NERC and Regional staff were undertaken on October 28, 2016. In these two sessions, Gartner provided an executive-level overview of the GRC space, then provided advice on the tool vendors under consideration. Gartner also reviewed our potential consulting partners (Deloitte and PricewaterhouseCoopers), including their placement within the Gartner Magic Quadrant for Risk Management Consulting Services.

NERC and the CMEP Steering Committee evaluated the potential consulting partners and ultimately selected Deloitte. The contract with Deloitte was executed on April 10, 2017, and initial work is beginning on this effort.

The next steps in this effort will be to conduct a formal Request for Proposal in Q4 2017 with the remaining vendors under consideration, and use a rigorous selection process to choose the platform best suited to meet the needs of the ERO Enterprise. The program team will solicit participation from the CMEP Steering Committee in the development of the RFP and the evaluation of the responses, and bring a final recommendation to the CMEP Executive Committee for review and approval.

Exhibit G – Situation Awareness for FERC, NERC, and the Regional Entities (SAFNR)

Overview

The Situation Awareness for FERC, NERC, and the Regional Entities (SAFNR) tool, initiated in February 2010, is a system composed of hardware, software, and communication (network) capabilities, providing near real-time information about the current operating conditions of the BPS. SAFNR provides valuable information from a wide-area view about BPS impacts from hurricanes, hot and cold weather extremes, and varying system conditions. However, NERC's Bulk Power System Awareness (BPSA) staff's ability to accurately understand BPS current conditions has declined over the years as the technology has aged. Enhancing SAFNR will incorporate functionality elements piloted during GridEx IV and address the recommendations from both the *GridEx IV Executive Tabletop* and *GridEx IV Distributed Play Lessons Learned Report.*

Background

NERC and the Regional Entities monitor operating conditions on the BPS in North America to maintain an awareness of situations that may impact or have the potential to impact the reliable operation of the grid. As called for in the ROP,[47] the Situation Awareness program enables NERC to initiate timely communications with key stakeholders, including Reliability Coordinators, FERC, Canadian and Mexican governmental agencies, the DHS, and the E-ISAC. Awareness of system events also enables NERC to identify risks for mitigation through its Events Analysis process, permits and promotes the development of lessons learned, and contributes to the ability to trend reliability performance. Similarly, FERC monitors conditions on the BPS in the United States for comparable purposes. Situation Awareness has three essential elements: the ability to perceive, comprehend, and then project that understanding into the future. More simply stated, it is the "What?", "So what?", and finally, "Now what?" regarding the status of the grid.

The system has the capability to include data for electric system facilities operating at 230 kV and above and generation units at 500 MW and above and provides near-real time situational awareness information, with data provided by Reliability Coordinators, Balancing Authorities, and Transmission Operators. SAFNR provides the ability to monitor and be aware of the current conditions and assess forecasted conditions on the BPS. The tool also supports the ability to understand and clearly communicate normal system conditions (or conditions of heightened risk to reliability) among Reliability Coordinators, Regional Entities, NERC and FERC.

SAFNR was procured using specifications and technology from 2010, making the technology platform quite dated relative to the latest available tools. With the insights and experience gained from the years of successful use, enhancements and advanced capabilities are envisioned for rapid and accurate situational awareness that protects the proprietary nature of the information while maximizing the understanding of the system conditions, especially during emergencies.

While a successful tool deployment has been maintained and used successfully for more than eight years, NERC BPSA staff cannot efficiently or cost effectively update the underlying power system information or real-time data feeds on risks to reliability, such as severe weather, flooding, and wildfires, as well as available information on interconnection frequency, Balancing Authority ACE, and aggregated customer outages. The tool has been used to support the GridEx exercise, but also demonstrated its shortcomings when aiming for a more precise wide-area view of system conditions. Enhancing SAFNR will incorporate functionality elements piloted during GridEx IV that

[47] Section 1000 contains NERC's responsibilities for Situation Awareness and Critical Infrastructure Protection (CIP), including its role as the E-ISAC. Additional expectations are outlined in Sections 807, 808, and 810 regarding analysis of events and the dissemination of lessons learned, advisories, recommendations, and essential actions.

provided the E-ISAC and the ESCC with more timely and understandable information. Further, these improvements address the *GridEx IV Executive Tabletop Report* recommendation that states that NERC and the E-ISAC should enhance their ability to provide reliable, timely, and accurate information regarding the state of grid reliability and security threats and events.

Next Steps

NERC IT's Project Management Office will guide this project through the normal process, including development of a business case, managing the RFP, negotiating with vendors and developers, and ultimately ensuring the successful implementation of the new tool This approach can be summarized as follows:

- Development of a business opportunity and assessment analysis
    - Current state and future state
- Financial analysis
    - Capital and operational costs
    - Return on investment
- Project governance and gated approvals
    - Executive sponsorship
    - Tollgates
    - Leadership review (e.g., ERO TLT)
    - Monthly financial review
- Project execution
    - Project management oversight
    - Project communications
    - Project scheduling and resource management
    - Contract/vendor management
- Change management and training
    - Regional and registered entity engagement and communications
    - Business value analysis and benefits realization

Appendix 1 – NERC Staff Organization Chart

The organizational chart is posted separately from the BP&B document for the first draft.