Xcel Energy®

414 Nicollet Mall
Minneapolis, MN 55401

January 17, 2020

—Via Electronic Filing—

Ryan Barlow
Acting Executive Secretary
Minnesota Public Utilities Commission
121 7th Place East, Suite 350
St. Paul, MN 55101

Re: Reply Comments
Distribution System – Hosting Capacity Analysis Report
Docket No. E002/M-19-685

Dear Mr. Barlow:

Northern States Power Company, doing business as Xcel Energy, submits the enclosed Reply Comments in response to the Comments received by parties on December 30, 2019 regarding our 2019 Hosting Capacity Analysis Report.

Pursuant to Minn. Stat. § 216.17, subd. 3, we have electronically filed this document with the Minnesota Public Utilities Commission, and copies have been served on all parties on the attached service lists. Please contact me at bria.e.shea@xcelenergy.com or 612-330-6064 if you have any questions regarding this filing.

Sincerely,

/s/

Bria E. Shea
Director, Regulatory & Strategic Analysis

Enclosures
c: Service List

STATE OF MINNESOTA
BEFORE THE
MINNESOTA PUBLIC UTILITIES COMMISSION

Katie J. Sieben	Chair
Valerie Means	Commissioner
Matthew Schuerger	Commissioner
John A. Tuma	Commissioner

IN THE MATTER OF THE XCEL ENERGY
2019 HOSTING CAPACITY REPORT
UNDER MINN. STAT. § 216B.2425, SUBD.
8

DOCKET NO. E002/M-19-685

REPLY COMMENTS

INTRODUCTION

Northern States Power Company, doing business as Xcel Energy, submits these Reply Comments in response to the Comments received by parties on December 30, 2019 regarding our 2019 Hosting Capacity Analysis (HCA) report.

We appreciate the Comments of the Minnesota Department of Commerce, Fresh Energy, and the Interstate Renewable Energy Council (IREC) and the recognition that we have significantly advanced our HCA report. With this report, we engaged more deeply with stakeholders and responded to their feedback – increasing the functionality of the Heat Map and making additional system detail available.

In this Reply, we provide the information requested by the Department and respond to parties' comments and questions regarding our 2019 HCA in the following areas: the frequency of analysis and relation to the interconnection process, grid and customer security, privacy and confidentiality, and stakeholder engagement.

Xcel Energy recognizes the hosting capacity analysis as an important part of system planning that contributes to Minnesota's public policy objectives for Distributed Energy Resources (DER). We are proud of the significant progress we have made to advance the value of the HCA report in a meaningful way to-date, which parties recognized in Comments. We have made these changes and advanced our HCA in response to the Commission and stakeholder feedback, learnings from the few other national utilities that are also doing this type of analysis, and our work with EPRI.

With our 2018 HCA, we observed that hosting capacity analysis was at a critical juncture where the Commission may need to further clarify the objectives of the HCA to avoid potentially conflicting objectives or misplaced expectations on future HCA reports. For our 2019 HCA, the Commission provided additional direction – and in response, we expanded the information we provide with our HCA results, and we more deeply engaged with developers and other stakeholders to better understand their expectations regarding how a hosting capacity analysis may be a more valuable precursor to the interconnection process. While stakeholder participation was lighter than we hoped, we appreciate the time and thoughtfulness stakeholders who participated in our workshop and survey dedicated to providing helpful and candid information and feedback to inform future analyses.

Some of the feedback we sought was regarding the frequency of hosting capacity analysis and its relation to Minnesota's statewide standard Distribution Interconnection Process (MN DIP) – specifically in relation to the information included in the current pre-application data report available in MN DIP. We took some steps to provide additional information currently provided only in the pre-application data report with our HCA, and in this Reply, we clarify further the challenges or concerns involved with providing other pre-application data with the HCA. We also commit to providing a full analysis of publishing HCA data more frequently – and, a full analysis of further integrating pre-application data into our 2020 HCA if the Commission agrees with the Department's recommendation that we develop a specific plan to integrate the pre-application data report and the HCA

That said, we believe our HCA continues to be at a critical juncture in terms of its role in helping Minnesota achieve public policies related to DER. We continue to believe that the HCA report is intended to provide insight as to potential feeder capacity, and is only *one tool among several* necessary to accommodate and integrate DER without causing adverse impacts on the distribution system.

We also believe there are important, relevant, and timely considerations of grid and customer security, privacy and confidentiality that must be factored into any future plans or directions for the HCA. As we explain in this Reply, fundamentally, just because a utility or another state is handling an issue or data differently does not make it wrong for another utility or state to do it differently – particularly in the case where grid and customer security and privacy hang in the balance, there must be a clear demonstration that the public interest outweighs the risks. The legislative and regulatory framework in Minnesota is not at this time driving to transform the utility paradigm and create markets for DER like it is in other leading HCA states, such that an argument for public disclosure of the data we have sought to protect would outweigh the security and privacy risks.

Further, since the time that certain public utilities commissions and/or individual utilities decided, deliberately or not, to publicly publish or otherwise provide distribution grid information, national security concerns have increased. The President's National Infrastructure Advisory Council, an executive council charged with examining cross-sector critical infrastructure security and resilience issues, issued a Report in December 2019 stating that "escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government economic stability, social order, and national security." The report continues and concludes saying "It is not a matter of if, but when, an attack will happen. Our window of opportunity to thwart a cyber 9-11 attack before it happens is closing quickly."

These threats are not just to our grid, and the impacts that may result to our customers and Minnesota generally – but also to the direct security of our customers. In addition to a number of our customers being part of the nation's and state's critical infrastructure, we expect all customers would have some level of economic, social, and/or other concerns for the security of their homes, businesses, and energy/utility service. Additionally, we are not convinced that customers would *want* the details of how their facilities connect to the distribution grid publicly revealed. So, in addition to the usage-related privacy concerns we discussed at length in our HCA filing, we believe the details of customers' grid connections themselves warrant cautionary treatment.

Fundamentally, our treatment of grid and customer data in the HCA is responsible, appropriate, and fully supported. We are happy to engage with the Commission in a further dialogue about grid data, and grid and customer security, privacy, and confidentiality. However, that discussion should involve all utilities, relevant experts with a role in protecting critical infrastructure, and customers. If that discussion does take place, it would be important that the discussion not provide a public road map on how to disrupt to the distribution system and service to customers.

Finally, we note our appreciation for the Department's analysis that synchronized the Commission's most recent Order requirements with the requirement to also provide the information required in past HCA Orders. To the extent the Commission decides to continue past requirements for our 2020 HCA, we respectfully request the

Commission to memorialize the specific requirements in relation to any new requirements that may intersect, such as the Department outlined in Comments.

In the balance of this Reply, we first focus on comments regarding our 2019 HCA report, and then discuss the comments regarding future hosting capacity analyses, security, privacy, and confidentiality considerations, and stakeholder engagement.

REPLY COMMENTS

I. 2019 HCA MODEL, RESULTS, AND ACCURACY

In this section we provide additional information about the comparison of DRIVE to other models and the mitigation solution analysis we performed. We also clarify some methodological details.

A. HCA Model Comparison

The August 2019 Order required the Company to provide an analysis of the DRIVE tool, which we provided in our HCA report on pages 5-6 of our Compliance filing and in Appendix A. The Department requested the Company to provide further information to support our analysis of comparing DRIVE to other methodologies and interconnection study results. Specifically, the Department requested that we explain the capabilities of Synergi and its role in fulfilling this requirement.

There are three established commercially-available tools that can conduct a hosting capacity analysis. They include Synergi, Cyme and DRIVE. In California, the Integrated Capacity Analysis (ICA) method uses two of those models to determine hosting capacity. PG&E and SCE used Cyme, while SDG&E uses Synergi. We compared DRIVE results to Synergi, because we have the Synergi software tool, and because it is a relevant comparison to what is being used with the ICA methodology in the industry. Our positive correlation with that tool also aligns with SDG&E's findings, which are highlighted in our report. We would not be able to do an actual comparison of tools that we do not maintain – including Cyme. We therefore paired our direct analysis with an EPRI report that compares the various methodologies being employed in the industry.

We believe the information we provided in our 2019 HCA fully responds to the Commission's directive in the August 2019 Order. Therefore, in response to the Department's recommendation that we repeat this analysis in our 2020 HCA report, we do not believe there is much to be gained by conducting a similar analysis. Rather, we suggest that we report any substantive HCA advancements or shifts that we observe in the industry in our 2020 HCA.

B. 2018 HCA Mitigation Options Analysis

Our 2018 HCA results showed 95 feeders with zero hosting capacity. The Commission's August 2019 Order required the Company to analyze these feeders in more detail to better understand how hosting capacity might be increased. In response to this requirement, we engaged EPRI – and, as discussed in our filing, were the first utility to use a new mitigation assessment tool they developed that allowed for a streamlined analysis of a large number of feeders. As we discuss below, without use of this tool, we would not have been able to complete this analysis in a timely manner.

First, we stress the complexity and novelty of this analysis. We believe this was one of the first attempts in the utility industry at automating a mitigation assessment for hosting capacity – an approach we believe was necessary given the nature of the analysis, the volume of feeders, and the compressed timeframe. We are fortunate we were able to partner with EPRI to utilize their cutting-edge advancements in this area. Still, we note that it took approximately 400 hours of their time to provide results for just the most cost-effective solution at *one* location for each feeder. Expanding the analysis to encompass *all* potential solutions would have exponentially increased the complexity and time, and would not have been completed in time to meet our filing deadline.

Instead of providing multiple specific solutions for each feeder, we provided seven typical mitigations used to solve voltage and thermal problems and three additional solutions to address any remaining issues. In our report we document approximate costs for those mitigations – and by focusing on the least cost alternative, it is apparent that all other options will be more expensive. Furthermore, we provided mitigation cost Tiers for the feeders with zero hosting capacity, which should help provide more insight on typical costs for the mitigations used. We believe this approach and information is consistent with our feedback and the resulting discussion at the hearing on our 2018 HCA report that resulted in the Ordering Point Nos. 3A and 3B of the Commission's August 15, 2019 Order. We also believe this additional discussion regarding our approach and analysis is also responsive to the Department's Request 4, which sought an explanation that establishes a reasonable basis for our approach in relation to the Department's reading of the Order requirements.

In response to Fresh Energy's questions about the mitigation tool and analysis, we note that we have not compared the results to actual interconnection studies, as it would require that the interconnection study was performed at the *exact* location that was assumed in the mitigation tool analysis (mid-point of the feeder). Consequently, this would make any error ranges, if produced as part of the tool, subjective without sound data for multiple locations. As we have previously stated, and as acknowledged by IREC, we also believe comparing the HCA results to actual interconnection studies provides limited value. We respond to Fresh Energy's questions about how the Advanced Planning Tool for which we proposed certification in our 2019 Integrated Distribution Plan will be used to improve the detail of the HCA in Section II.I below.[1]

C. Sub-Feeder Defined

Fresh Energy requested we explain how sub-feeder is defined, and whether we apply the definition consistently for every feeder. Generally, "sub-feeder results" means that the results are more granular than for an entire feeder. The sub-feeder results contained in our 2019 HCA are based off of section, or "nodal" results produced by DRIVE. In an effort to make the Heat Map practically useful, we combine nodal results into sections. We do this consistently for every feeder and break down the colors on the heat map according to the values displayed in the legend.

D. Daytime Minimum Load

Finally, we clarify the daytime minimum load (DML) information we portrayed in our 2019 HCA report was only partially based on actual DML information. On page 5 of our compliance filing, we outlined the improvements we made to our 2019 HCA compared to previous iterations. While we stated that the DML information used in our analysis was actual DML results for 25 percent of our feeders, we did not make clear that the balance of DML information for our system was based on estimated DML. As we have explained in previously HCA reports, we are only able to obtain actual DML information for the portion of feeders on our system equipped with Supervisory Data Access and Control (SCADA) capabilities.[2] The description of the DML information used in our analysis should have read as follows, with changes noted in red font:

- *Use of Actual Daytime Minimum Load (DML) Data*: We determined actual DML data for every feeder with large amounts of existing DER, where possible. As a result, we used actual DML values for approximately 25 percent of feeders in

[1] *See* Xcel Energy IDP, Docket No. E002/M-19-666 (November 1, 2019).

[2] Approximately 60 percent of our substations have SCADA and these substations serve approximately 90 percent of our customers.

the DRIVE analysis.[3] We continued to establish actual DML values during the rest of the HCA process for the rest of the SCADA-enabled feeders on our system~~, and feeders in the heat map and tabular results spreadsheet have DML data~~. The *majority* of the DML values are *actual* DML values, with the remaining being approximations based on a percentage of the known peak.

II. FUTURE HOSTING CAPACITY ANALYSES

All parties suggested the HCA be conducted or updated more frequently than its current annual cycle, and also that the HCA be further integrated with the current pre-application data report step of the Interconnection Process – or to better understand what that might involve. There was also interest in the granularity of the information presented to users, and the potential expansion of the current DER generation hosting capacity analysis to a system load analysis. This is consistent with feedback presented during our stakeholder discussions in September 2019.

A. Role of HCA in Relation to Interconnection Process

Minnesota is a leader in terms of requiring HCA. In other leading states however, public policies surrounding DER are often an outcome of shifts in the regulatory paradigm, and in some cases – namely California and New York – public policies intended to develop or further competitive DER markets. While Minnesota too has public policies supporting increased deployment of DER – and the Commission is taking action to further those policies – the circumstances in Minnesota are different.

For example, in 2017 the California Legislature enacted legislation to further California's commitment to reducing greenhouse gas emissions and deploying DER – and the California Commission has been actively considering augmentations and refinements to many of DER policies in Commission proceedings over a significant period of time. The 2017 Legislative DER action plan was intended to align the Commission's vision and actions to shape California's DER future.[4] One of the vision elements for DER to meet grid needs through a transparent, seamless planning and sourcing process that (1) removes barriers for utilities, (2) establishes DER sourcing mechanisms, and (3) recognizes DER cost-effectiveness and valuation frameworks that reflect full grid services – and includes supporting attributes, including improved hosting capacity estimates that minimize the need for

[3] This includes some feeders without DER for which we had previously determined actual DML.

[4] *See*https://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/About_Us/Organization/Commissioners/Michael_J._Picker/DER%20Action%20Plan%20(5-3-17)%20CLEAN.pdf

interconnection studies and ensure greater cost certainty, and streamlining of utility application practices.

Specifically related to the integration of HCA with the interconnection process, in Minnesota, we have a different regulatory framework established by state statute. For example, the Commission just recently concluded a proceeding that established a standard statewide process for interconnection (Minnesota Distribution Interconnection Process, or MN DIP) in Docket No. E999/CI-16-521. By statute (Minn. Stat. § 216B.1611), this is the uniform statewide process for processing distributed generation interconnection applications. The MN DIP process controls where interconnection studies are needed, and does not include hosting capacity as part of this process. Our interconnection tariff contains the new MN DIP requirements. This includes MN DIP 1.4, the "Pre-Application Report Request" at tariff sheets 10-172 to 10-175, and sheets 10-211 to 10-212, that includes a fee of $300 for information in that report.

We believe there must be a balance between resource investment, public policy drivers, and the public interest. While we agree there may be value in deepening the hosting capacity analysis to more closely align with the first step of the MN DIP process, we believe that may go beyond the current statutory provisions for HCA and perhaps other legislative frameworks. We clarify that a pre-application data report is an opportunity to get early guidance signals of potential capacity for a substation or feeder to accommodate a specific DER project. It is fee-based, to recognize the resources required to perform the analysis, and aligned cost-causation principles. By its nature, a pre-application data report is a preliminary analysis of a *specific project* at a *specific location* on our system at a *specific point in time*. The current fee for a pre-application report is $300. Conversely, a hosting capacity analysis is a *generalized* analysis of the entire system that estimates the amount of DER that might be able to be accommodated at *anywhere on the system* without the need for system upgrades at the time of the analysis – and is free.

Increasing the depth and/or breadth of the HCA to replicate or replace the need for the MN DIP pre-application report process will necessarily increase the resources required to perform the analysis. It also raises the question as to whether all customers should pay for that level of analysis, or whether potential interconnecting customers should bear the cost for gaining that information, as they do today under cost-causation principles.

That said, if the Commission agrees with the Department's recommendation that we develop a specific plan to integrate the pre-application data report and the HCA, we will provide it in conjunction with our 2020 HCA.

B. Frequency of Hosting Capacity Analysis

Comments generally observed that the HCA results would be more useful and actionable if the analysis were completed more frequently and if based on more granular information, with specific suggestions for improvements in both of these areas. The Department specifically requested that we develop and provide in our Reply a proposal to provide more frequent HCA updates at specific intervals. In this section, we address the comments regarding the frequency of the analysis.

The Department requested we provide a proposal for monthly, quarterly, and semi-annual HCA updates in our Reply Comments, including the costs associated with each frequency, and whether and how any additional costs can be imposed on those who obtain a benefit from more frequent updates. We note that we are not able to fully develop such a proposal in the Reply timeframe. We will however, provide a full analysis and proposal with our 2020 HCA filing.

Below, we outline what we believe are key factors and/or considerations that will impact our ability and/or the cost of providing HCA information more frequently than the current annual cycle.

- *Full or partial update.* A significant determinant of resources and thus costs will be whether it is necessary to perform an analysis of our full distribution system more frequently or if targeted updates will produce reasonably accurate results.
- *Criteria to determine partial updates.* If it is determined targeted, or partial, updates will produce the expected level of results, the criteria used to determine when updates are appropriate and what specifically requires updating will have a significant impact on the resource requirements and costs.
- *The desired update frequency.* In addition to the scope of the analysis as noted above, the cadence of the updated HCA reports will be a significant driver of resource requirements and costs.

As we have explained, we currently produce the HCA within our Distribution Planning team using the same team of engineers that are responsible for integrated distribution planning and other system planning work. We currently rely heavily on summer interns to complete portions of the analysis, which works with the current November 1 annual report timing. We also rely on workgroups outside of the Distribution function, including our Geospatial Information Systems team, who converts the HCA results into the Heat Map. While we agree with IREC's and Fresh Energy's suggestions that targeted updates where changes are occurring on the distribution system may reduce the overall cost of more frequent HCA reports, at this time, we believe our current process and resources would not be sufficient to conduct multiple full or partial analyses throughout the year. That said, as noted above, we will provide our analysis in conjunction with our 2020 HCA report.

Finally, we note that IREC states that a best practice for HCA is more frequent updates than annual. While we agree that a more frequent cadence of HCA information would increase the accuracy and relevance of the information, a best practice rooted in non-traditional regulatory paradigms may not directly transfer to Minnesota. Thus, we reiterate our belief that the associated resource investment must be commensurate with public policy drivers and consistent with cost causation principles.

C. Granularity of HCA Analysis and Results

Comments generally observed that the HCA results would be more useful and actionable if the analysis were completed more frequently and if based on more granular information, with specific suggestions for improvements in both of these areas. In this section, we address the comments regarding the granularity of the analysis and results.

1. Daytime Minimum Load

IREC suggested the Company perform HCA analyses using two different DML values to avoid seasonal constraints on our system – one it believes would produce more useful data for customers seeking to design a photovoltaic (PV) systems and another for other systems. And, ultimately that we should move toward providing hourly HCA results using the 24 hour load profile of each month's peak day and minimum day.

As it stands today, hosting capacity analysis is performed under two conditions: (1) peak loading, and (2) minimum loading. We perform the analysis at each node on the feeder, increasing in 100kW steps until one of the constraints is violated. Using a rough estimate of 3,000 nodes per feeder and an average hosting capacity of 1 MW of

DER on the system, this is 10 iterations at 3,000 nodes for two different conditions – or approximately 60,000 calculations per feeder.

Moving toward a monthly peak day and minimum day analysis would be considered a "576 Analysis" and would increase the number calculations performed for hosting capacity analysis by 288 times – for a total of approximately 17,280,000 calculations per feeder.[5]

This is an exponential increase in the amount of processing power and data management that would be needed to perform such an analysis. We do not believe the limited benefit this analysis would provide in any way is balanced with the overwhelming effort required to perform such an analysis.

Further, the data required to perform such an analysis is not readily available in the areas for which it would provide the most benefit. At current, the vast majority of the Solar*Rewards Community (S*RC) gardens are located in the more rural areas the Company serves. These rural areas are less likely to have the SCADA data necessary develop the curves required to perform a 576 Analysis.

While we agree performing the additional analysis at absolute minimum loading could provide additional value for DER other than solar, we are not currently seeing levels of DER interconnection request activity of this type that would support this effort in the near-term or foreseeable future. Therefore, the Commission should reject IREC's recommendation that the Commission order the Company to provide monthly results using DML for the benefit of customers designing PV-only systems and absolute minimum load for the benefit of customers designing other systems

2. *Correlation of Heat Map and Tabular Results*

IREC Comments recognize that our production of HCA results on a line segment level is valuable over providing the results on a whole feeder basis. IREC also observes that our tabular spreadsheet provides a range of the hosting capacity of an entire feeder, which is a more summarized view of available hosting capacity on the system.

We present the tabular results by feeder to provide a more digestible summary of the detailed Heat Map. The minimum and maximum hosting capacities provided in the

[5] A "576 Analysis" refers to the fact that 576 hourly load profiles would be used (Peak and minimum day for each month, derived as follows: (24 hours)*(2 peak/min values)*(12 months)=576 hours. Because we already perform one analysis, we divided the 576 hours by 2 to derive the applicable multiplier (576/2=288).

tabular results are valuable pieces of information for each feeder. While they may not specifically point out *where* on a particular feeder the capacity is, these values make it easier to compare results year-over-year, and are good proxies for a feeder's ability to host more DER overall.

Our Heat Map shows in more detail what hosting capacity is available at certain locations and in our view, is the best way to gain this information. We believe providing a spreadsheet for over a thousand feeders with thousands of nodes per feeder would be cumbersome, at best, for individuals to utilize and overly complicate the tabular results.

We reiterate that we view hosting capacity as a high level, no-cost-to-users, optional first step in the interconnection process, which aligns with our provision of a Heat Map and the information provided in the tabular results. We believe providing full nodal information in either spreadsheet or map form would provide a false sense of precision that should only be obtained through an actual interconnection study for a specific location.

3. Criteria Violation Values

IREC observed that publishing more granular hosting capacity results, including all the criteria violation values for each line segment, would provide customers with more meaningful and actionable information about the electric system than our current practice of providing only one-limiting criteria violation for the most restrictive value.

The specific criteria violation values are available in DRIVE. We have to-date chosen to summarize as minimum and maximum values for practicability/usability purposes in our tabular results. The varying minimum values can also be seen in more granularity through the pop-ups in the online map. We appreciate the suggestion that more granularity in this area would provide additional value to users. We will examine how we might be able to further increase the granularity while preserving usability, and discuss the results of our examination in our next HCA.

We also note however, that this is not as straightforward as it may sound. The system is dynamic and any action taken can affect the next action. Using IREC's example where Primary-Over-Voltage is the first limiting element at 500 kW, and Thermal for Discharging DER is the next limiting element at 750 kW, the second element/the thermal violation may be affected by whatever mitigation is chosen to solve the first element/the voltage violation. For example, if power factor correction is chosen to solve the Primary-Over-Voltage condition, the Thermal for Discharging DER value could become more restrictive as a result. Conversely, if reconductoring is chosen as the first mitigation, the 750 kW value may become larger and not be an issue at all.

In summary, while it may appear on the surface that providing more information is a good idea, it is essential to consider the practical usefulness of the information. In some situations such as this, the additional information may not be useful or actionable, and could even be misleading. We will however, examine how we might be able to increase the granularity of this information in a way that maintains its practicable usability, and discuss the results of our examination in our next HCA.

D. Expanding HCA to Consider Load

Fresh Energy noted two types of load-related analyses it believes are important to begin to incorporate into the HCA sooner than later: (1) modeling hosting capacity, as currently done, with the addition of load characteristics of DERs installed at the time of modeling, and (2) modeling hosting capacity under various scenarios of DER deployment, including both generation and load DERs. Fresh Energy noted that the first may not be critical to do until deployment levels warrant, but that it sees the second as important for informing integrated distribution planning and identifying comprehensive mitigations for areas of limited hosting capacity. IREC similarly suggested expanding the HCA analysis to consider load DER – and a distinct load analysis comparable to the current hosting capacity analysis, which it also suggested may provide value in conjunction with integrated distribution planning and investments. Finally, the Department suggested that perhaps the Commission desired more than we provided in our 2019 HCA regarding DRIVE's ability to possibly assist with state energy policy goals related to beneficial electrification.

1. *Adding Load DER to the Current HCA*

We believe load characteristics of DER are best handled within the distribution planning/study process where load has always been the focus, and should not be brought into the annual HCA filing where the focus is generation capabilities.

There would be little to no benefit provided by adding load based DER to the HCA. Adding load to allow for the installation of more DER generation has at most, little more than a one-to-one effect on the system – and depending on load characteristics, could be less. This means that for every one MW of load added, the hosting capacity at that location can be increased by one MW at most. The one exception to this is in the circumstance where the added load is consuming VARs, which aids in reducing the localized voltage. This is the concept behind using power factor mitigation on generating DER installations. Increasing the power factor mitigation applied to a generating DER would have the same effect in boosting the localized hosting capacity. However, drawing additional VARs beyond current limits is not an advised approach, because VARs have to be generated somewhere – and that cost is borne by customers, not generators. Finally, generation equipment has limited power factor operating ranges, and power factor mitigation has a diminishing return.

To provide relevant and usable information about an increase in hosting capacity due to a change in load requires specific information about the load's operational characteristics. Without this information, the analysis would be theoretical in nature, and thus would provide no practicable or usable information beyond the generic potential for a one-to-one increase, as discussed above. In summary, we do not believe this sort of analysis will provide the broad benefits that parties are looking for, and that this information is better placed within our existing distribution planning/study process(es).

2. *Distinct Distribution System Load Analysis*

IREC suggests that a load analysis for hosting capacity purposes can provide important insight for the Commission and other stakeholders as they review and approve long-term integrated distribution plans and investments, with the aim to integrate these resources in the lowest cost manner for the benefit of all ratepayers.

We perform a system load analysis as part of our annual system planning process, as described in the Integrated Distribution Plan (IDP), most recently filed on November 1, 2019 in Docket No. E002/M-19-666. As also described in the IDP, we also perform load analyses throughout the year as we become aware of changes on the system, either Company- or customer-driven. These analyses are essential to ensure we continue to provide our customers with safe, reliable service.

Performing a load analysis requires a different set of inputs than a generating hosting capacity analysis. With generating hosting capacity, the worst case scenario is at light loading times with high voltage. A loading analysis worst case scenario is at heavy loading with low voltage. In short, this would be a different analysis that would have to be analyzed separately from the generation hosting capacity. Also as discussed further in the Security and Privacy Considerations section of this Reply, publishing a load map would compromise grid security and customer privacy and security.

We agree the software tools we employ for our HCA and system analyses (i.e., DRIVE and Synergi, among others) can perform this load analysis – and that hosting and other system planning will increasingly integrate. However, we believe load analysis and planning – and assessment of distribution system investments – are appropriately separate and apart from an annual hosting capacity analysis and not contemplated by the current legislative framework. In the case of a load analysis for purposes of informing public policy discussions and decisions regarding beneficial electrification, we believe a focused and specific analysis would be necessary – after engaging with appropriate stakeholders on the scope, objectives, assumptions, and inputs. We are open to further discussion about performing such a study if the Commission believes it will be helpful toward state energy policy goals.

E. Potential for Load DER as a Mitigation Option

As far as Fresh Energy's request to include load DER as potential mitigation options in the DRIVE tool, as discussed in Part D above, several technical concerns will need to be resolved before we can consider load DER as viable mitigation options. Further, we clarify that the mitigation assessment is not part of DRIVE. We are open to requesting EPRI to add load DER into their Mitigation Assessment Tool as a potential mitigation alternative; we are not however, able to guarantee EPRI will make that change, as we are only one of a number of stakeholders with input and making suggestions for its future direction. We will however report in our 2020 HCA the results of our discussion with EPRI. Finally, assuming the technical concerns can be resolved, for the results to be valid, there would need to be an analysis on how the location, timing and extent that the load aligns with the location, timing and extent of generation of the DER.

F. Ongoing Accuracy Assessments

In Comments, IREC observed that our 2019 HCA's accuracy check is a good start, but that additional data validation efforts will be needed once frequency and granularity issues are addressed.

Today, some of the quality checks we perform are comparing the minimum and maximum hosting capacities and the limiting threshold of each feeder to the previous year's minimum and maximum hosting capacities and limiting thresholds to identify potential anomalies or outliers that require additional analysis. If there are large discrepancies or differing thresholds, we flag them for further engineering review. We also specifically flag all of the feeders with zero hosting capacity even if no change occurred year to year, and assess the potential reasons for the zero value. We believe these will continue to be important parts of the analysis.

We have also conducted analyses of HCA results compared to the results from specific interconnection studies. We appreciate IREC's agreement and recognition in Comments that comparing interconnection studies to HCA results has limited value.

This was again evidenced by the results of our analysis that showed the differences in HCA-Interconnection Study results has more to do with the HCA model update frequency and less granular analysis than the accuracy of the HCA model.

We agree it will be important to establish an ongoing plan to ensure accuracy of the HCA results once the framework, parameters, and objectives for the ongoing HCA are confirmed and/or modified.

G. Secondary System Data

Fresh Energy requested information about the new combined DRIVE method, whether it relies on secondary system data, and if so how Advanced Metering Infrastructure (AMI) might aid the collection of the secondary system data.

First, we clarify that the combined DRIVE method is a hybrid of the Large Centralized and the Small Distributed Methodologies. At this point, we believe this combined approach will – in one step – provide the answer to the hosting limitations on the primary system, whether caused by centralized or distributed DER. DRIVE is focused on the complex analysis of the hosting capacities of the primary system, rather than localized secondary capacity restrictions, which are better and more efficiently addressed individually.

SAMI meters can measure values such as voltage, current, frequency, real and reactive power, and certain power quality events. For hosting capacity, the most relevant ones are voltage and power. Voltage insights will help us observe with more granularity, where we have high or low voltage on the distribution system – and whether the concern is widespread or localized. The power values will help us better tune our Advanced Distribution Management System (ADMS) models, which will offer a comparison to our hosting capacity models.

Beyond these standard AMI features, as discussed in our AGIS certification request, we are also planning Distributed Intelligence capabilities. These capabilities offer enhanced field analysis, some of which could improve hosting capacity results and our understanding of them. We have not finalized our implementation plans at this point, but they may include functionality such as the following:

- Improved security and awareness,
- Energy usage control and savings,
- Smarter insights about customer energy data and information,
- Smarter controls to better manage and integrate different systems, and
- Identification and alarming for operational issues.

More work needs to be done to determine how we will fully leverage all of the data and capabilities, including Distributed Intelligence, for maximum benefit for our customers. This includes integrations with other systems and potentially new tools to view and interact with the data. Our AMI timeline for Minnesota is currently proposed to begin in 2021 and go through 2024. We look forward to further discussions and dialogue with the Commission and stakeholders about these plans. We also note that we are planning a stakeholder workshop on the combined DRIVE methodology in the first quarter of 2020 when we more fully understand its capabilities and the potential benefits and/or pitfalls, and where we will be able to answer further questions such as this.

H. Sensitivity Analysis

The Department requested that we discuss whether it might be valuable to perform sensitivity analysis on variables other than that we have conducted previously in our next HCA. We note that the sensitivity analysis we have produced to-date has been for two of the most impactful factors (voltage and power factor). We have also produced an analysis that shows the effect of load and generation on hosting capacity for various locations. At this time, the only other factor we believe we could potentially adjust would be the increment at which we add generation to the model in our analysis. While we could do more iterations with more increments, it would not alter the hosting capacity significantly; it would essentially just provide a more granular value. We therefore believe there is limited value in adding this to the HCA analysis at this time, and that our resources are better focused on more substantive advancements such as potentially increasing the frequency of the analysis.

I. Role of our Proposed Advanced Planning Tool with HCA

One of the major benefits of the APT that we believe will directly improve the HCA is its ability to better forecast load. When implemented fully, we plan to use the APT to generate the load forecasts that we will use in our HCA. While we plan to do scenario analysis with the APT as part of our overall system planning, we believe at this point in time, carrying those scenarios over into the HCA would be very time consuming, as a separate analysis would be needed for each scenario. With today's tools and capabilities, this would result in hundreds to thousands of additional hours, with just the addition of a few extra scenarios. We are hopeful that as these tools mature, we will be able to more efficiently perform these types of analyses on a more wholistic basis for our system.

III. SECURITY, PRIVACY, AND CONFIDENTIALITY

Since first providing the Heat Map with our annual HCA report, we have raised and discussed what we believe are serious grid security and customer privacy and security concerns associated with providing a public-facing map of our distribution system. We again addressed security and privacy considerations in our 2019 HCA report both generally, and specific to new Order requirements from the Commission.

One of the new Order requirements was to provide peak load information for both feeders and substation transformers. The Company provided this information with not public designation(s) under the Minnesota Data Practices Act for security reasons, and also explained that stakeholders had not identified peak load data as necessary to the usefulness of the HCA information. The Department's Comments agreed with the Company that the security risks of publicly providing peak substation transformer and/or feeder load data outweigh the public interest in making the data publicly available.

The Company also redacted certain information from the public-facing Heat Map for security and privacy reasons. The Department assessed the substantive information the Commission's Order required the Company to provide in the event it withheld information for security or privacy reasons, and concluded that the Company complied with the Commission's requirements to describe and provide a specific basis for withholding the information.

Fresh Energy asked the Company to respond to questions regarding the comparability of legal frameworks in other states where at least some utilities provide more detailed grid information. IREC asserted that the Company did not sufficiently support the actions it took in the interest of grid security and customer privacy and security. We address these questions and concerns below.

A. Regulatory Frameworks are a Relevant Consideration

By all accounts, California and New York are leading the nation in regulatory proceedings to create a marketplace opportunity for renewable and distributed generation. According to a Utility Dive article[6] summarizing the activity as of April 2018, The New York Reforming the Energy Vision (REV) was into its third year and second phase, and spanning at least 16 major proceedings, along with the investor-owned utilities' rate cases; at that time, there were also four related proceedings, as well as proceedings at the New York State Energy Research and Development Authority and the Federal Energy Regulatory Commission. The California Public Utility Commission's (CPUC) work on DER had evolved into 12 major proceedings as well as those overseen by the California Energy Commission and the California Independent System Operator. The CPUC last year published a seven-page DER Action Plan summarizing its efforts into three categories and 15 "strategic directives" with four "objectives" through 2018. The NY Public Service Commission (PSC) was at that time working on a roadmap for REV intended to offer the same overview.

These proceedings are working to transform each state's power supply, part of which is to facilitate the entry of third party DER providers into the market through an alternative regulatory structure. It stands to reason that this type of legislative and regulatory shift in the utility paradigm may drive differing treatment of grid and customer data to serve those public policies. Our HCA filing discussed that California utilities were ordered to provide certain grid information in support of legislative and regulatory frameworks designed to create and facilitate a California DER market. As also discussed in our HCA filing, those utilities have since petitioned the Commission to discontinue the practice of publicly providing detailed distribution grid information after becoming aware foreign entities were downloading large amounts of that data. The utilities' petition is still pending, and Administrative Law Judges were co-assigned to the docket on October 25, 2019.[7]

Fundamentally, just because a utility or another state is handling an issue or data differently does not make it wrong for another utility or state to do it differently. Particularly in the case where grid and customer security and privacy hang in the

[6] *See* https://www.utilitydive.com/news/unnecessary-complexity-assessing-new-york-and-californias-landmark-der-pr/514748/

[7] *See* October 25, 2019 Notice of Co-Assignment of ALJs. The filings in that docket can be accessed here: https://apps.cpuc.ca.gov/apex/f?p=401:57:0::NO

balance, there must be a clear demonstration that the public interest outweighs the risks. We believe the legislative and regulatory framework in Minnesota is not at this time driving to transform the utility paradigm and create markets for DER, such that an argument for public disclosure of the data we have sought to protect would outweigh the security and privacy risks. Further, even if there were clear and apparent public policy drivers in Minnesota comparable to California and New York, we believe a fresh look at decisions as to what information is publicly provided is necessary, which we discuss in Part B below.

B. Critical Infrastructure Threats and Risks are Increasing

Since the time that certain public utilities commissions and/or individual utilities decided, deliberately or not, to publicly publish or otherwise provide distribution grid information, national security concerns have increased.

The California utilities' case noted in part 1 above demonstrates that the threat of nation states gathering information about the United States' critical infrastructure is real and tangible. A December 9, 2019 article in The Hill titled *Federal council to Trump: Cyber threats pose 'existential threat' to the nation* summarizes what was at the time a draft report from the President's National Infrastructure Advisory Council (NIAC).[8] NIAC is the only executive council that examines cross-sector critical infrastructure security and resilience issues and provides recommendations to the President on how to secure the nation's infrastructure.[9] The Council includes up to 30 senior executives appointed from across the critical infrastructure sectors, including finance, health, and energy, who draw upon their deep experience, engage national experts, and conduct

[8] *See* https://thehill.com/policy/cybersecurity/473682-federal-council-to-trump-cyber-threats-pose-existential-threat-to-the

[9] *See* https://www.cisa.gov/national-infrastructure-advisory-council

extensive research to discern the key insights that lead to practical federal solutions to complex problems.

NIAC finalized and issued its Report December 12, 2019, which boldly states that "escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government economic stability, social order, and national security."[10]

We highlight some of the relevant excerpts, primarily from pages 5-6 of the final report, below and provide the final report as Attachment A to this Reply:

> ## Compelling Case for Urgent Action
>
> The 2019 Worldwide Threat Assessment of the U.S. Intelligence Community paints an ominous picture of cyber threats to U.S. critical infrastructure:[11]
>
> - *China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.*
> - *Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting **an electrical distribution network** for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016.*
>   - ***Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.***
> - *Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017.*
>
> The nation risks unprecedented catastrophic failure of critical functions due to our increasing reliance on cyber systems that underpin nearly every aspect of commerce and our daily lives. Recent cyber attacks demonstrate growing capabilities for adversaries to disrupt critical infrastructure from thousands of miles away. These include the cyber attack on a nuclear plant in India in September 2019,[12] a March 2019 denial-of-service attack on wind and solar generating facilities in the United States,[13] the breach of a U.S. nuclear power plant's network in 2017,[14] the 2017 NotPetya attack that

[10] *See* https://www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf

[11] Daniel R. Coats, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," Before the Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[12] Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," *The Washington Post*, November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

[13] Robert Walton, "First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say," *Utility Dive*, November 4, 2019, https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.

[14] Sonam Sheth, "Hackers breached a US nuclear power plant's network, and it could be a 'big danger,'" *Business Insider,* June 29, 2017, https://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6.

> affected systems in multiple sectors throughout the world,[15] and the 2015 and 2016 cyber attacks on Ukraine's electric grid.[16]
>
> **The need to act is urgent:**
>
> 1. **Nation-states and other well-resourced adversaries have intensified their efforts to infiltrate and gain control of the cyber networks of key U.S. critical infrastructures (energy—specifically electricity and natural gas,** financial services, and communications), which are vital for continuity of government, public safety, economic stability, and national security.
> 2. Private sector companies are on the front lines of a cyber war they are ill-equipped to fully understand, thwart, or counter against nation-states intent upon disrupting and destroying critical infrastructure. Protecting national security from nation-states is not a part of their operating model.
> 3. Despite massive capabilities and investment across government and the private sector, the nation has been unable to rapidly harness and direct resources to mitigate the most serious cyber threats facing these key infrastructures.
> 4. Executive-driven public-private partnership is the most effective way to ensure joint action and mobilize resources to implement solutions in the private sector. Existing structures have not yet been effective in addressing the most urgent and dangerous cyber risks.
> 5. **It is not a matter of if, but when, an attack will happen. Our window of opportunity to thwart a cyber 9-11 attack before it happens is closing quickly**. [Emphasis added]

We note that since NIAC issued this call for urgent action, there is a general awareness that threat levels have further increased in the wake of U.S. actions with Iran.

These threats are not just to our grid, and the impacts that may result to our customers and Minnesota generally – but also to the direct security of our customers. In addition to a number of our customers being part of the nation's and state's critical infrastructure, we expect all customers would have some level of economic, social, and/or other concerns for the security of their homes, businesses, and energy/utility service.

IREC's suggestion that our Heat Map should be a detailed map that clearly portrays each line and each connection to substations, other utilities, and customer facilities is irresponsible. IREC argues that individuals can create such a map from public sources and/or drive around and create such a map. That may be so, and we cannot

[15] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[16] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

stop an individual or entity from taking such action. However, there is no compelling policy or other reason for the Company to make the information readily available.

Finally, in addition to the demonstrated security concerns, we are not convinced that customers would *want* the details of how their facilities connect to the distribution grid publicly revealed. So, in addition to the usage-related privacy concerns we discussed at length in our HCA filing, we believe the details of customers' grid connections themselves warrant cautionary treatment.

We have not responded to all of IREC's arguments, and note that some, including asking whether FERC has designed the information we maintain is not-public as Critical Energy Infrastructure Information (CEII), are not relevant.[17] Fundamentally, our treatment of grid and customer data in the HCA is responsible, appropriate, and fully supported. We are happy to engage with the Commission in a further dialogue about grid data, and grid and customer security, privacy, and confidentiality. However, that discussion should involve all utilities, relevant experts with a role in protecting critical infrastructure, and customers. If that discussion does take place, it would be important that the discussion not provide a public road map on how to disrupt to the distribution system and service to our customers.

IV. STAKEHOLDER ENGAGEMENT

The Department requested that we outline a preliminary plan to identify and engage additional stakeholders for involvement in the Company's next iteration of the HCA. The Department also requested that we explain the feasibility of the stakeholder suggestions and requests noted in our filing related to improving the public-hosting capacity map.

A. Preliminary Stakeholder Engagement Plan – 2020 HCA

We appreciate the feedback provided by stakeholders regarding their continued commitment to engaging in our hosting capacity analysis and process. We recognize that in order to incorporate stakeholder feedback into our future HCA iterations, we will need to engage stakeholders sooner than we have in the past, which has largely waited until the Commission has taken action on the current HCA.

To respond to the Department Comments regarding our level of stakeholder engagement on our 2019 HCA, we note that we notified and invited the most recent

[17] FERC's CEII designation and processes apply only to grid assets governed by FERC, which does not include the distribution system.

HCA docket service list and over 500 individuals that receive ongoing communications regarding interconnection of DER for our planned stakeholder meeting and survey. We additionally discussed the annual HCA at our Solar*Rewards Community Implementation Workgroup in an effort to generate interest and participation in the stakeholder meeting and survey. We also held our post-stakeholder meeting survey open much longer than originally planned – and issued several reminders encouraging everyone to participate and help shape the future direction of the HCA.

While the turn-out at our stakeholder meeting and response to our survey was less than we hoped, we believe it was not due to a lack of communication or effort on our part; it may have more to do with the fact that stakeholder engagement on this topic is relatively new. For 2020, we intend to start earlier and are hopeful that our communications, informal engagement with stakeholders, and demonstrated action based on feedback will spur more interest and participation.

For 2020, we plan to begin stakeholder outreach in the early-March timeframe to first engage on the new DRIVE combined methodology. We are taking action now to better understand its capabilities and what might be involved in using it for our 2020 HCA. We are excited to share this information with stakeholders and seek input from their technical experts on the potential benefits and implications of employing it in our next HCA.

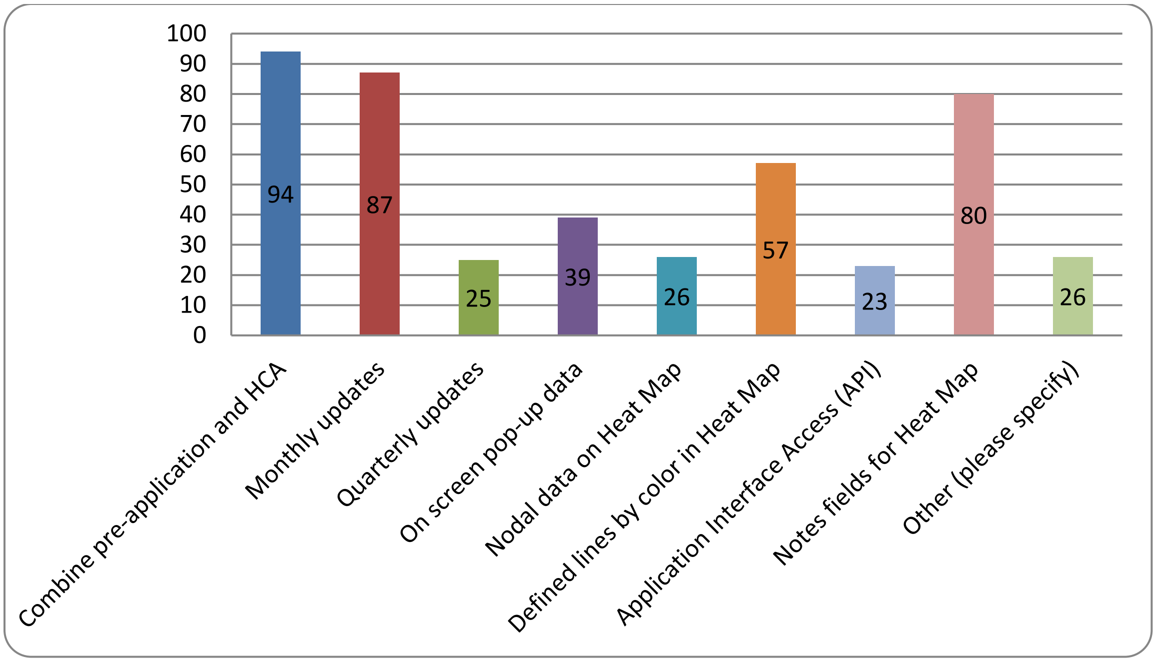
We envision a second stakeholder session in the April/May timeframe where we would engage on the technical assumptions and inputs used in our HCA, and engage more deeply on the HCA tools (Heat Map and tabular results). For example, to dig more deeply into the information the 2019 survey respondents suggested may be helpful in a "notes" box on the Heat Map. Fresh Energy requested whether we may be able to discuss the potential benefits of future AMI capabilities to the HCA. We have provided some information about that in this Reply and note that many of those details are yet to be determined. We are however open to starting that discussion in the second stakeholder session, and envision this will be an ongoing dialogue as our AMI and other proposed advanced grid investments play out over the next several years.

B. Stakeholder Feedback – Feasibility

In this section we respond to the Department's request that we: (1) respond to each of the stakeholder suggestions and requests listed in Figure 2 of our initial filing, and (2) the responses to our stakeholder and developer survey, explaining the feasibility of each of the items related to improving the public-hosting capacity map. For reference, we provide Figure 2 from our initial filing below.

The question asked survey participants: "During our September 6, 2019 Workshop, the Company received feedback to change *the functionality* of the Hosting Capacity process. Please rank the FIVE most important of these changes in siting your DER interconnection."

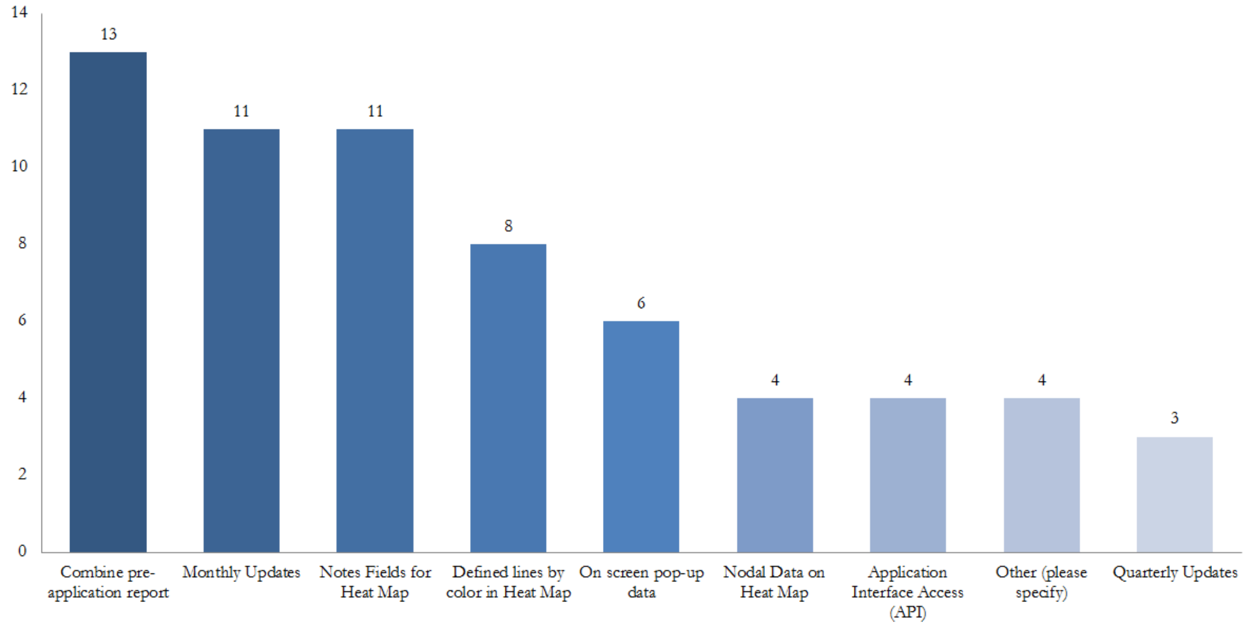
Figure [Initial Filing] 2: Rank the FIVE Most Important Functionality Changes for the HCA (Reported by Rank Score)



We clarify that the "Rank Score" is not representative of the number of responses or "votes" participants made for each functionality. As noted above, while we sent the survey to over 500 individuals involved or interested in the interconnection process and/or hosting capacity analysis, only three percent – or 15 individuals – responded to the survey.

We portray the actual "votes" for each functionality in Figure 1 below:

Figure 1: Rank the FIVE Most Important Functionality Changes for the HCA (Reported by Stakeholder Interest)



The results showed that stakeholders would like the future functionality to include the ability to combine the HCA with the pre-application report provided to interconnection applicants, more frequent updates to the Heat Map (monthly or quarterly), the addition of notes fields, more defined lines by color rather than a heat map (like GoogleMaps), pop-up data, additional nodal data and application interface access. Other respondents ranked items such as: accuracy, real data and size and length of conductors.

The majority of the 15 respondents – nearly all – would like to see the hosting capacity (1) combined with the pre-application report, (2) have the details updated monthly, and (3) include notes fields for further information. We provide the tabular data in Table 1 below, along with a brief assessment of feasibility.

Table 1: High Level Feasibility Assessment of Ranked Functionality Changes

Responses	Functionality Change	Feasibility Assessment
13	Combine pre-application and HCA	Reviewing for 2020 HCA
11	Monthly updates	Reviewing for 2020 HCA
11	Notes fields for Heat Map	Reviewing for 2020 HCA
8	Defined lines by color in Heat Map	Implicates security and privacy risks if provided at this level of detail
6	On-screen pop-up data	Added in 2019
4	Nodal data on Heat Map	There are approximately 3,000- 4,000 nodes per feeder. While not fully nodal level, we already provide sub-feeder level information. Given that very few stakeholders ranked this as a priority we have not moved forward with this suggestion at this time.
4	Other (please specify)	Other requests included accuracy, real data and size and length of conductors. We would include these details as part of the first three functionality changes.
4	Application Interface Access (API). *Note: API is an electronic data exchange protocol.*	Given very few stakeholders ranked this as a priority we have no moved forward with this suggestion at this time.
3	Quarterly updates	See "Monthly Updates."

We note that we are focused on the items with the greatest interest and impact, which we discuss in more detail below.

1. *Combining the HCA with the Pre-Application Report*

Stakeholders would like to see the HCA combined with the pre-application report instead of the current two separate processes and sets of data. With the changes we made with our 2019 HCA, more than half of the items provided in the pre-application data report can now be viewed directly or derived from the Heat Map. The remaining items are either impractical to provide on a broad basis through the HCA, or present security and privacy concerns as outlined in Table 9 of Attachment A, Hosting Capacity Analysis Report – Pages 45-46, to our HCA filing, with additional information provided in our response to IREC Information Request No. 6.[18]

Further, the HCA and pre-application data reports are not duplicative, nor intended to be duplicative, of each other. Rather, each has its own distinct purpose by design.

[18] See our response to IREC IR No. 6 in Attachment A to IREC's December 30, 2019 Comments in this docket.

HCA should provide a generalized analysis of all locations, while the pre-application report is for a specific project at a specific point in time. As we described earlier in this Reply, the type of analysis needed to determine how these two reports could be combined and how costs should be allocated is much more extensive than time allowed for this Reply. We will therefore address it more fully in our 2020 HCA report.

2. *Update the HCA Monthly*

We continue to explore ways to update the HCA on a more frequent interval, as discussed earlier in this Reply. We will provide the analysis the Department requested, in which we will also explore targeted/partial updates, in our 2020 HCA report.

3. *Notes Field*

Stakeholders would like to see notes fields in the HCA describing such things as whether the feeder is near capacity, or if there is a limiting factor such as Voltage Fluctuation. We were not able to implement this request as part of our 2019 HCA, given the time involved in assessing the types of data suggested – and the effort necessary to gather the data and modify our processes and systems to provide the functionality. We are continuing to examine this for potential inclusion in our 2020 HCA; however, we believe there would be value in discussing this in more detail with a broader group of stakeholders to define specifically the information that would be most helpful – as our survey did not go into that much detail, and despite our best efforts to prompt responses, it only had 15 respondents. We have therefore included this in our stakeholder engagement plan outlined in Part A above.

We also briefly address the request for the hosting capacity map to be more like Google Maps instead of in a heat map form. Providing a specific and detailed map of our distribution assets, grid, and customer connections presents privacy and security risks as discussed in our filing and Section III of this Reply.

We recognize that stakeholder engagement is a key component of ensuring our HCA is a useful tool for identifying potential areas on our distribution grid where additional DER may be sited, before initiating the first step of the interconnection process with a specific project. We made a strong effort in 2019 to engage relevant stakeholders toward helping to identify potential enhancements or future directions for hosting capacity analysis in Minnesota. Participation was less than we would have hoped, but the stakeholders who participated were excited, engaged, and provided very helpful information, which we appreciate. For 2020, we have identified and outlined several topics where we intend to engage stakeholders, beginning in the early-Spring timeframe. We will discuss the results of our work with stakeholders in our 2020 HCA.

CONCLUSION

Xcel Energy respectfully requests that the Commission accept our 2019 Hosting Capacity Analysis. The Company further requests that the Commission clarify any ongoing reporting requirements as outlined by the Department in Comments.

Dated: January 17, 2020

Northern States Power Company

NIAC The President's National Infrastructure Advisory Council

December 12, 2019

The Honorable Donald J. Trump
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC

Dear Mr. President,

On September 5, 2019, the National Security Council tasked the President's National Infrastructure Advisory Council (NIAC) to examine how the federal government and private industry can collaborate seamlessly to confront urgent cyber risks in the most critical and highly targeted private infrastructure.

Mr. President, escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win against nation-states intent on disrupting or destroying our critical infrastructure. **Bold action is needed to prevent the dire consequences of a catastrophic cyber attack on energy, communication, and financial infrastructures.**

The nation is not sufficiently organized to counter the aggressive tactics used by our adversaries to infiltrate, map, deny, disrupt, and destroy sensitive cyber systems in the private sector. To fix this, the Council recommends the following actions:

Make Cyber Intelligence Actionable

1. Establish the Critical Infrastructure Command Center (CICC) to improve the real-time sharing and processing of private and public data—including classified information—between co-located government intelligence analysts and cyber experts with clearances from companies and functions at greatest risk (Section 9(a), E.O. 13800). The CICC will foster the trust and collaboration essential to develop the actionable intelligence and threat mitigations needed to counter rapidly evolving threats to our nation's critical infrastructure.
2. Direct the Intelligence Community to raise the priority of collecting, detecting, identifying, disseminating, and rapidly declassifying information on efforts by nation-state and non-state actors to exploit or otherwise attack critical infrastructure in the United States. This should be a Priority 1 topic within the National Intelligence Priorities Framework as a critical part of our national security.
3. Conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to CEOs of identified energy, communications, and financial services companies to build a compelling case for company action to counter serious cyber threats and to facilitate operationalizing the CICC.
4. Use the upcoming National Level Exercise 2020 to pilot the CICC model by bringing together cleared private sector experts with intelligence officers and representatives from other key government agencies, such as law enforcement and sector-specific agencies, to collaboratively analyze classified threats and understand resulting consequences to critical infrastructure.

Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission

5. Issue an Executive Order to create the Federal Cybersecurity Commission (FCSC) as an independent U.S. government entity to mitigate catastrophic cyber risks to critical infrastructure that have potential

national security impacts. The Commission offers a bold new approach for the streamlining of regulatory authorities to achieve cyber mitigations in the private sector and counter extraordinary cyber threats, in consultation with an executive partnership of industry executives and government leaders.

6. Convene a symposium of select Cabinet Secretaries, regulators, Office of Management and Budget (OMB) officials, CEOs, and industry representatives to clarify the functions, roles, responsibilities, and processes of the Commission, based on the more detailed work done by the NIAC.

Modernize Legal Authorities to Improve Cyber Defense

7. Direct the Department of Justice to analyze existing legal authorities: 1) to determine the ability of government to direct the private sector to implement cyber mitigations, and 2) to identify legal barriers that prevent the private sector from implementing requested mitigations and sharing information with the government.

Secure the Supply Chain of Critical Cyber Components

8. Provide liability protection to allow blacklisting and whitelisting of critical cyber products used in private critical infrastructure, similar to the authority provided in 10 CFR Part 21 for the nuclear industry and to the Department of Energy's (DOE) enhanced procurement authority.
9. Continue and expand programs at the DOE's national laboratories and other ongoing initiatives by each sector to independently test vendor equipment for vulnerabilities and report the results to private companies.

Mr. President, America's companies are fighting a cyber war against multi-billion-dollar nation-state cyber forces that they cannot win on their own. Incremental steps are no longer sufficient; bold approaches must be taken. Your leadership is needed to provide companies with the intelligence, resources, and legal protection necessary to win this war and avoid the dire consequences of losing it. Establishing the CICC and FCSC will empower our nation to meet, engage, and thwart those who choose to target our critical infrastructure.

On behalf of our fellow NIAC members, we thank you for the opportunity to serve our country through participation in this Council. We stand ready to provide additional details and discussion about this important subject.

Wallace

Michael J. Wallace
Former Vice Chairman and
COO, Constellation Energy
Working Group Member

William J. Fehrman
President and CEO,
Berkshire Hathaway Energy
Working Group Member

J. Rich Baich
CISO,
AIG, Inc.
Working Group Member

Richard H. Ledgett, Jr.
Former Deputy Director,
National Security Agency
Working Group Member

Connie

Constance Lau
President and CEO
Hawaiian Electric Industries, Inc.
NIAC Chair

Beverly

Dr. Beverly Scott
CEO
Beverly Scott Associates, LLC
NIAC Vice Chair

NIAC The President's National Infrastructure Advisory Council

Transforming the U.S. Cyber Threat Partnership

December 2019

Table of Contents

About the NIAC

The President's National Infrastructure Advisory Council (NIAC) is composed of senior executives from industry and state and local government who own and operate the critical infrastructure essential to modern life. The Council was established by executive order in October 2001 to advise the President on practical strategies for industry and government to reduce complex risks to the designated critical infrastructure sectors.

At the President's request, NIAC members conduct in-depth studies on physical and cyber risks to critical infrastructure and recommend solutions that reduce risks and improve security and resilience. Members draw upon their deep experience, engage national experts, and conduct extensive research to discern the key insights that lead to practical federal solutions to complex problems.

For more information on the NIAC and its work, please visit: https://www.cisa.gov/niac

National Security Council Tasking and Study Scope

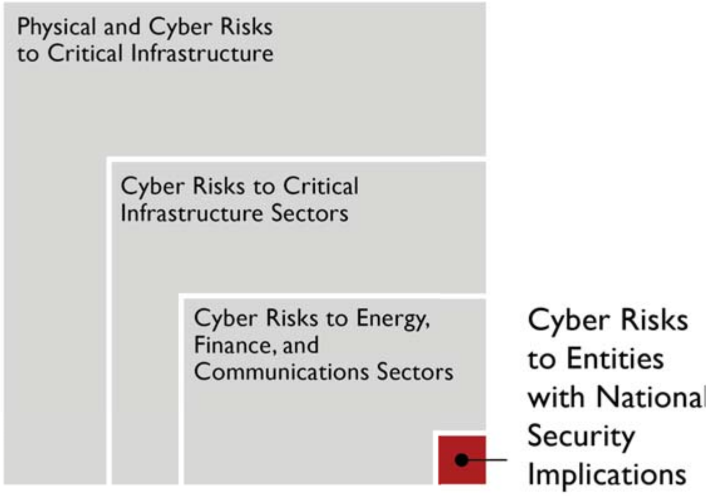
Escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. This conclusion is supported by a wealth of prior studies, including those conducted by the NIAC, the National Security Telecommunications Advisory Committee, the Commission on Enhancing National Cybersecurity, and the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community. Despite the many actions taken to date, current efforts have not produced the bold steps needed to properly defend our most critical assets, causing us to fall further behind.

On September 5, 2019, the National Security Council tasked the NIAC to examine how the federal government and private industry can collaborate seamlessly to manage urgent cyber risks in the most critical and highly targeted private infrastructures. A Working Group of four NIAC members was formed to complete the task. For the purposes of this study, references to the private sector or companies encompass any infrastructure that is not federally owned and/or operated.

Given the severity of current cyber threats and the multitude of challenges in addressing them, the Working Group focused on how to protect the most at-risk entities and functions within the energy, financial services, and communications sectors (Figure 1). A disruptive cyber attack on key assets within these sectors could result in catastrophic regional or national effects on public health and safety, economic security, or national security.[1]

This fast-track effort built on the foundation of prior studies and recommendations, classified threat briefings, and the Working Group members' experiences, and did not require the extensive research conducted for other NIAC studies (see Appendix C for a list of prior studies and references). The Working Group conducted three in-person work sessions with senior government and industry leaders to gather input and insights to inform its recommendations (see Appendix B for a list of contributors). The Working Group supplemented these discussions with focused research and interviews with experts.

Figure 1. Study Scope


Physical and Cyber Risks to Critical Infrastructure
Cyber Risks to Critical Infrastructure Sectors
Cyber Risks to Energy, Finance, and Communications Sectors
Cyber Risks to Entities with National Security Implications

The study's narrow focus is not intended to conflict with or replace ongoing initiatives to improve cybersecurity in all sectors or other efforts to increase coordination and partnership between sectors and government.

[1] Executive Office of the President, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (E.O. 13800)," May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Compelling Case for Urgent Action

The 2019 Worldwide Threat Assessment of the U.S. Intelligence Community paints an ominous picture of cyber threats to U.S. critical infrastructure:[2]

- *China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States.*
- *Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016.*
    - *Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.*
- *Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017.*

The nation risks unprecedented catastrophic failure of critical functions due to our increasing reliance on cyber systems that underpin nearly every aspect of commerce and our daily lives. Recent cyber attacks demonstrate growing capabilities for adversaries to disrupt critical infrastructure from thousands of miles away. These include the cyber attack on a nuclear plant in India in September 2019,[3] a March 2019 denial-of-service attack on wind and solar generating facilities in the United States,[4] the breach of a U.S. nuclear power plant's network in 2017,[5] the 2017 NotPetya attack that affected systems in multiple sectors throughout the world,[6] and the 2015 and 2016 cyber attacks on Ukraine's electric grid.[7]

The need to act is urgent:

1. Nation-states and other well-resourced adversaries have intensified their efforts to infiltrate and gain control of the cyber networks of key U.S. critical infrastructures (energy—specifically electricity and natural gas, financial services, and communications), which are vital for continuity of government, public safety, economic stability, and national security.

2. Private sector companies are on the front lines of a cyber war they are ill-equipped to fully understand, thwart, or counter against nation-states intent upon disrupting and destroying critical infrastructure. Protecting national security from nation-states is not a part of their operating model.

[2] Daniel R. Coats, "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," Before the Senate Select Committee on Intelligence, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[3] Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," *The Washington Post*, November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

[4] Robert Walton, "First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say," *Utility Dive*, November 4, 2019, https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.

[5] Sonam Sheth, "Hackers breached a US nuclear power plant's network, and it could be a 'big danger,'" *Business Insider,* June 29, 2017, https://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6.

[6] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[7] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

3. Despite massive capabilities and investment across government and the private sector, the nation has been unable to rapidly harness and direct resources to mitigate the most serious cyber threats facing these key infrastructures.

4. Executive-driven public-private partnership is the most effective way to ensure joint action and mobilize resources to implement solutions in the private sector. Existing structures have not yet been effective in addressing the most urgent and dangerous cyber risks.

5. It is not a matter of if, but when, an attack will happen. **Our window of opportunity to thwart a cyber 9-11 attack before it happens is closing quickly**.

Fundamental Principles

The NIAC's recommendations are predicated on a set of fundamental principles that affirm the shared responsibility of government and industry to protect U.S. critical infrastructure.

1. **Industry and government must partner to protect our critical infrastructure** from nation-state attacks to ensure the security and common defense of the United States. This shared responsibility requires that government help defend private infrastructure from sophisticated cyber attacks just as it defends against nuclear attacks.
2. **Priority should be placed on the most critical infrastructures that underpin national security** and other critical functions, with the ability to expand the model to defend other critical infrastructure, and then the nation writ large. The approach must be adaptable to enable cost-effective participation of small- and medium-sized enterprises, which may have limited technical or financial resources to achieve the same level of protection.
3. **The private sector cost to achieve national security objectives is beyond that required to meet normal commercial interests**. The government has a responsibility to provide appropriate channels to compensate companies for implementing extraordinary measures of cyber protection, including through federal tax relief, cost sharing, regulatory cost recovery approval, or other methods.
4. **The private sector has a responsibility to help the government understand the implications of cyber risks to company systems.** Attacks in cyberspace happen at network speed, and our processes and methods must correspond to this reality. The private sector and the government must communicate information in real time to enable them to react, respond to, and mitigate cyber threats.
5. **Making cybersecurity intelligence/information actionable allows government and industry to effectively defend the country at network speed.** This approach is not intended as a substitute or replacement of existing cybersecurity standards (e.g., National Institute of Standards and Technology Cybersecurity Framework) that improve cyber hygiene throughout critical infrastructure. Rather, it recognizes that the government must prioritize severe national cyber risks and accelerate the sharing of threat information to enable private companies to mitigate risks at machine speed.
6. **A provision to regulate industry actions must exist as a last resort to ensure necessary cyber protection against extraordinary nation-state threats.** Voluntary action, supported by incentives and market mechanisms, is the most desirable and effective way to achieve private sector cybersecurity. However, certain regulatory powers must be available to the U.S. government to protect critical national infrastructures and systems in extreme circumstances to ensure national security. In some cases, regulations may provide certain legal protections needed for commercial operations.

Urgent and Comprehensive Approach

Incremental cybersecurity improvements cannot keep pace with the rapid, asymmetric offensive strategies used by nation-states to infiltrate, map, and compromise the cyber networks of U.S. critical infrastructure. The past 20 years of well-meaning government efforts have shown that our national approach to securing the cyber assets of critical infrastructure is far less than optimal. Radical new approaches are needed that combine the extensive capabilities and resources of government and industry to protect private sector networks where failure could result in catastrophic impacts on public safety, economic stability, and national security.

New models that realign traditional public and private sector roles and responsibilities will likely require new legislation that will take time to implement—time we do not have.

The NIAC recommends a two-track approach:

1) **URGENT Action**: Pursue solutions that address urgent, near-term cyber risks that have national security implications and that can be implemented rapidly using existing authorities.
2) **COMPREHENSIVE Solution**: Design the ideal model for an assured measure of protection informed by an executive-driven public-private partnership. This approach would likely require legislation.

We recognize that bold new approaches that realign established responsibilities and programs in the federal government are hard to achieve. Building support among affected stakeholders and gaining consensus to act take time and resolve. But we must begin working toward the ideal long-term solution now. We also cannot ignore the urgent security threats that our critical infrastructure owners and operators face today. Our two-track approach ensures that we address the urgent needs of today while working toward a sustainable long-term solution.

Strategies and Recommendations

Four strategies are needed to respond to catastrophic cyber risks to the energy, communications, and financial services sectors: 1) Make Cyber Intelligence Actionable, 2) Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission, 3) Modernize Legal Authorities to Improve Cyber Defense, and 4) Secure the Supply Chain of Sensitive Cyber Components. The NIAC developed specific recommendations to achieve each of these strategies.

Make Cyber Intelligence Actionable

Company access to classified threats to company cyber infrastructure is vital for mitigating risks. However, intelligence information sharing is impeded by three key factors: 1) insufficient clearances for private sector managers, 2) limited understanding of how a cyber threat could disrupt, disable, or damage a company's enterprise, and 3) delays in translating aggressive cyber threats into actionable mitigations.

These factors limit the ability of the federal government to provide clarity on the magnitude of the risk and the steps companies must take to mitigate risks to their systems in a timely manner.

Recommendations

1. **Establish the Critical Infrastructure Command Center (CICC)** to improve the real-time sharing and processing of private and public data—including classified information—between co-located government intelligence analysts, cyber experts with clearances from companies and functions at greatest risk (Section 9(a), E.O. 13800), and key government agencies, including sector-specific agencies, law enforcement, and the intelligence community. The CICC will foster the trust and collaboration essential to develop the actionable intelligence and threat mitigations needed to counter rapidly evolving threats to our nation's critical infrastructure.

    a. Company and government intelligence and cyber experts would work side-by-side at a 24/7 watch floor to receive cyber threat information in real-time, understand implications of that threat for company systems (and more broadly national security, economic stability, and public safety), and enable company-specific and sector-wide mitigation actions.

    b. Participating companies would provide cleared personnel to staff the watch floor, including individuals with a broad understanding of company assets and experience with rapid executive decision making. Such personnel would have appropriate access to the company systems.

    c. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) should lead the development of the CICC in its role as the central department for sharing cybersecurity information between government and industry authorized under the Cybersecurity Information Sharing Act of 2015.

    d. In time, the bi-directional information sharing of the CICC should become multi-directional, so that what is learned in one sector flows rapidly to others.

2. **Direct the Intelligence Community to raise the priority** of collecting, detecting, identifying, disseminating, and rapidly declassifying information on efforts by nation-state and non-state actors to exploit or otherwise attack critical infrastructure in the United States. This should be a Priority 1 topic within the National Intelligence Priorities Framework as a critical part of our national security.

3. **Conduct a one-day Top Secret/Sensitive Compartmented Information (TS/SCI) briefing to CEOs** of identified energy, communications, and financial services companies to build a compelling case for company action to counter serious cyber threats and to facilitate operationalizing the CICC.
    a. The briefing is intended only for the companies identified to be part of the CICC to reinforce the need for immediate action.
4. **Use the upcoming National Level Exercise (NLE) 2020 to pilot the CICC model** by bringing together cleared private sector experts with intelligence officers and representatives from other key government agencies, such as law enforcement and sector-specific agencies, to collaboratively analyze classified threats and understand resulting consequences to critical infrastructure.
    a. The NLE is based on real-world incidents and brings together thousands of individuals from across all levels of government and the private sector. The NLE would be an opportunity for the agencies most directly involved in the CICC—DHS, Department of Energy (DOE), Department of the Treasury, Department of Defense (DOD), and Federal Communications Commission (FCC)—to identify how the model could be used to identify and mitigate cyber risks for the most at-risk entities and functions identified.

Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission

There is a growing recognition that government institutions have not been organized and optimized to help address cybersecurity threats from nation-state adversaries (and those that act like them) who are intent on disrupting or destroying private critical infrastructure. As a result, it is often unclear where private sector owners and operators should turn to obtain information and assistance from the government in addressing and responding to urgent cyber threats.

The Council believes that the severity and speed of international cyber threats demand a new, centralized approach that allows businesses and government to integrate real-time information, determine actions needed by both the private sector and the government, respond at network speed, and bring to bear the expertise, capabilities, and authorities of federal agencies.

Recommendations

5. **Issue an Executive Order to create the Federal Cybersecurity Commission (FCSC)** as an independent U.S. government entity to mitigate catastrophic cyber risks to critical infrastructure that have potential national security impacts. The Commission offers a bold new approach for the streamlining of regulatory authorities to achieve cyber mitigations in the private sector and counter extraordinary cyber threats, in consultation with an executive partnership of industry executives and government leaders.
    a. The FCSC would not replace existing regulatory and oversight agencies. Rather, it would serve as a bridge between the government and the identified companies in the energy, financial services, and communications sectors to help mitigate the most urgent cyber issues. For other federal agencies, the FCSC would provide cyber expertise and potentially serve as a clearinghouse for cyber-related issues in the three sectors (see Appendix A for a full description).

6. **Convene a symposium** of select Cabinet Secretaries, regulators, Office of Management and Budget (OMB) officials, CEOs, and industry representatives to clarify the functions, roles, responsibilities, and processes of the Commission, based on the work done by the NIAC.

    a. Creating a new federal entity requires in-depth discussions with invested stakeholders to ensure that the FCSC is not duplicating efforts and that it has the scope intended by the NIAC. The symposium is an opportunity to gather broader input to ensure the ultimate success of the Commission.

    b. While the creation of the FCSC could be accomplished by executive order, legislation will likely be required to provide the Commission with the authorities and funding needed to be fully operational. The President should include the FCSC in his budget submission to Congress.

Modernize Legal Authorities to Improve Cyber Defense

Many of our nation's laws and regulations could not have envisioned the way cyber systems and networks would underpin and connect our most critical infrastructure functions. In some ways, these laws and regulations have hindered proactive cybersecurity efforts by diverting company resources to comply with outdated regulations at the expense of more cutting-edge cybersecurity investments to counter emerging threats. New laws and regulations have created a patchwork of authorities that in some cases has not been applied in real-world situations.

The NIAC found in its 2017 *Securing Cyber Assets* study that the federal government has tremendous capabilities and authorities, but these are scattered across a wide swath of agencies, departments, and sub-units.[8] Private sector companies require legal clarity before they can apply resources to measures that could prevent or mitigate cyber attacks.

Recommendations

7. **Direct the Department of Justice** to analyze existing legal authorities: 1) to determine the ability of government to direct the private sector to implement cyber mitigations, and 2) to identify legal barriers that prevent the private sector from implementing requested mitigations and sharing information with the government.

    a. An initial analysis conducted by the Working Group indicates that the Defense Production Act, the Federal Power Act, and the SAFETY Act all contain provisions that could enable the government to direct cyber mitigations in critical infrastructure sectors and provide liability protections to companies that implement certain technologies. However, more guidance and interpretation from the federal government is needed to understand the extent of these powers and under what circumstances they could be used in response to nation-state cyber threats.

[8] National Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Threats to Critical Infrastructure*, August 2017, https://www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf.

Secure the Supply Chain of Critical Cyber Components

Hardware, software, and service providers rely on a complex international supply chain that at times has allowed nation-states to introduce components and malware into digital equipment used in critical infrastructures. Compromised components provide adversaries with a foothold into company networks and systems that allows them to map, control, and ultimately disrupt or destroy critical functions.

Under the National Defense Authorization Act for Fiscal Year 2014, the Secretary of Energy has the authority to use classified threat information to end contracts or eliminate companies from contract competitions without providing cause if it is based on classified information.[9] To our knowledge, the DOE has yet to use this authority.

Voluntary efforts and initiatives exist today to improve supply chain security of information and communications technology. The federal government has supply chain risk management practices and standards required for federal procurement. However, voluntary standards and leveraging federal guidelines are not enough to protect the most highly targeted and at-risk companies.

Existing cyber attack reporting requirements are not supply-chain specific and do not appear to limit the liability of an entity reporting information. The ability to share information on security issues with devices and components would be a step toward helping companies shore up security within the supply chain. Current laws and regulations do not adequately support this type of information sharing between companies.

Recommendations

8. **Provide liability protection to allow blacklisting and whitelisting** of critical cyber products used in private critical infrastructure, similar to the authority provided in 10 CFR Part 21 for the nuclear industry and to the DOE's enhanced procurement authority.
9. **Continue and expand programs at the DOE's national laboratories** and other ongoing initiatives by each sector to independently test vendor equipment for vulnerabilities and report the results to private companies.
    a. A key role the federal government can play is the independent testing and validating of vendor equipment.
    b. The NIAC supports ongoing initiatives and working groups focused on supply chain, including the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, and would encourage their continuation and expansion.

[9] U.S. Government Accountability Office, "Nuclear Supply Chain: NNSA Should Notify Congress of its Recommendations to Improve the Enhanced Procurement Authority," August 8, 2019, https://www.gao.gov/assets/710/700794.pdf.

Call to Action

The White House must move swiftly to implement our two-track approach:

1) **URGENT Action:** Pursue solutions that address urgent, near-term cyber risks that have national security implications and that can be implemented rapidly.

2) **COMPREHENSIVE Solution:** Design the ideal model for an assured measure of protection informed by an executive-driven public-private partnership. This approach would likely require legislation.

The time to act is now. The President should immediately appoint a senior leader to oversee the implementation of recommendations in this report.

The NIAC stands ready to continue to support the President in this area, and will continue to follow developments closely, so as to provide timely follow-up perspectives to the President, as appropriate. Moreover, we recommend that a status update on the recommendations in this report be provided to the NIAC within three months, including the actions being taken and planned to implement these recommendations.

Escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. We need to act now.

Appendix A: Federal Cybersecurity Commission

The protection of critical infrastructure is a shared responsibility between industry and government that has grown more important as nation-states and non-state actors seek to infiltrate private sector cyber networks with the intent to disrupt and destroy them. Today, the federal government is not effectively organized to reflect this new paradigm, in which public and private partners must quickly share intelligence about cyber threats and have clear authorities and lines of communications to respond to cyber attacks at network speed. Existing gaps and overlaps in cybersecurity responsibilities among government entities and between government and the private sector create the potential for misunderstanding, miscommunication, and lapses in cyber protection, detection, and response.

Mission

The Federal Cybersecurity Commission (FCSC) is proposed as an independent U.S. government agency, overseen by Congress, dedicated to mitigating catastrophic cyber risks to the most targeted and critical private infrastructure companies, whose failure could threaten national security. A key feature of the FCSC is that it will have limited regulatory authority and will work in close collaboration with an executive-driven public-private partnership represented by senior executives from relevant industry and government entities.

Vision

The long-term vision of the FCSC will be to ensure the confidentiality, integrity, and availability of cyber systems used in private sector critical infrastructure, where failure could result in catastrophic impacts on national security, public safety, and economic stability for the United States.

Scope

The efforts of the FCSC will be narrowly focused on a small number of critically important infrastructures and assets in the private sector. The FCSC will:

- Focus on three vitally important sectors—**energy** (electricity and natural gas), **communications**, and **financial services**—which underpin the operations of other critical infrastructures and functions.
- Focus on the most at-risk entities and/or functions within these critical infrastructures that would have national security consequences if they were to fail.
- Focus on cyber threats by nation-state and non-state actors to exploit, deny, or otherwise attack these critical infrastructures to bring about consequences that threaten national security.

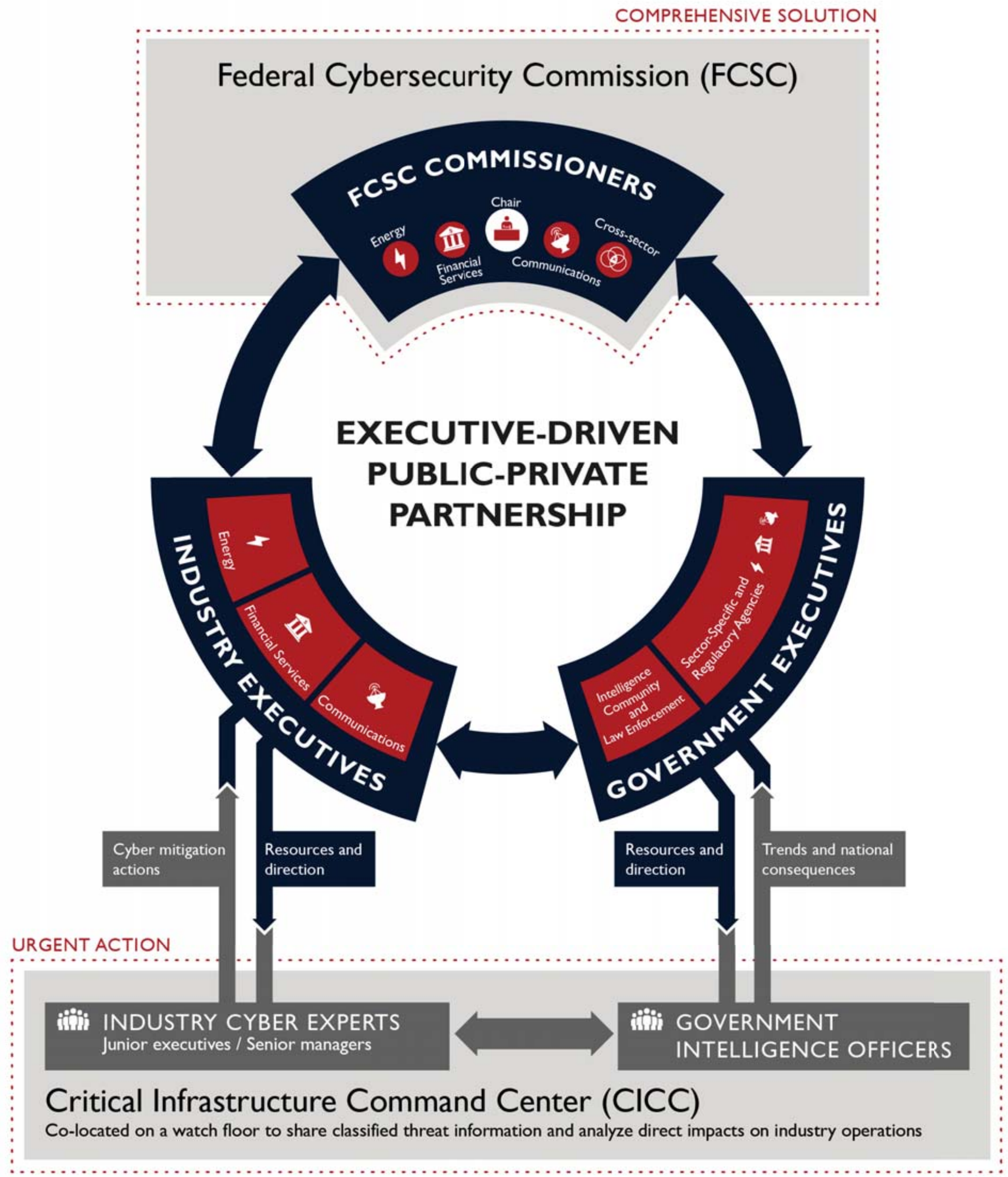
Roles

The FCSC bridges the distinct roles and responsibilities of the federal government and the private sector, which must be unified when attacks on private infrastructure equate to attacks on the nation. The FCSC provides the structure and necessary authorities to:

- Rapidly identify and direct companies to implement industry-led mitigations to counter severe cyber threats (including preventive/protective measures and response/recovery measures).
- Provide liability protection to private companies that act on mitigation measures as directed to thwart attacks.

- Accelerate intelligence sharing and analysis of nation-state threats to industry-owned systems, leveraging the CICC.
- Advise on government response to identified infrastructure threats.
- Set standards, rules, and/or regulations to ensure information technology (IT) and operational technology (OT) equipment and supply chain integrity.
- Harmonize conflicting or duplicative regulations that impede cybersecurity.
- Provide a last-resort regulatory backstop to ensure critical measures are implemented.

Figure 2. FCSC Structure


COMPREHENSIVE SOLUTION
Federal Cybersecurity Commission (FCSC)
FCSC COMMISSIONERS
Energy
Financial Services
Chair
Communications
Cross-sector
EXECUTIVE-DRIVEN
PUBLIC-PRIVATE
PARTNERSHIP
INDUSTRY EXECUTIVES
Energy
Financial Services
Communications
GOVERNMENT EXECUTIVES
Sector-Specific and Regulatory Agencies
Intelligence Community and Law Enforcement
Cyber mitigation actions
Resources and direction
Resources and direction
Trends and national consequences
URGENT ACTION
INDUSTRY CYBER EXPERTS
Junior executives / Senior managers
GOVERNMENT INTELLIGENCE OFFICERS
Critical Infrastructure Command Center (CICC)
Co-located on a watch floor to share classified threat information and analyze direct impacts on industry operations

Structure and People

The FCSC will be the convener, coordinator, central clearinghouse, and regulator as a last resort for cybersecurity efforts for these most at-risk entities. To be effective, it must work collaboratively with an executive-driven public-private partnership composed of senior leaders from the three sectors and key federal agencies (Figure 2). It must also draw upon and act on intelligence and infrastructure impact information from the CICC.

Under the FCSC, private sector and government executives are expected to act collaboratively, quickly, proactively, and decisively to serious and immediate threats to critical infrastructure assets or functions to meet national security needs, while respecting the roles and responsibilities of each side of the partnership.

FCSC Commissioners

The FCSC will be led by five Commissioners: three sector-specific commissioners (energy, financial services, and communications), one cross-sector commissioner, and one chair. Commissioners will have ultimate authority over rules and actions needed to mitigate cyber risks in private sector infrastructure that have severe national security impacts. Commissioners will be appointed by the President.

Responsibilities

- Direct the expert technical and administrative staff to help assess, communicate, and implement necessary industry actions to ensure compliance with cyber mitigations in the private sector that are deemed to be essential for ensuring national security.
- Develop particularly close working relationships with key U.S. government entities, including the Intelligence Community, DOD, relevant sector agencies (e.g., DOE), law enforcement, and others in order to assure a timely and complete understanding of the threat environment.

FCSC Staff

The Staff will be headed by an Executive Director who will lead, manage, and direct the activities of a full-time legal, technical, policy, and administrative staff that executes the direction and decisions of the Commission. The staff should also include rotating detailees—experienced junior executives/senior managers drawn from both the private sector and from key government agencies—who bring sector-specific expertise or represent the cybersecurity, intelligence, and law enforcement communities. Such individuals could be detailed for a limited period of time (e.g., less than two years).

Responsibilities:

- Receive input from the CICC and from government and private sector leaders on all matters, including vulnerabilities, threats, potential impacts, risks of actions by adversaries, or risks inherent in the critical infrastructure.
- Analyze developments and risks potentially impacting the private sector infrastructure.
- Recommend policy measures, regulatory actions, and guidelines to the Commission in situations where no existing federal authorities or mechanisms exist to ensure the security of critical cyber systems.
- Carry out directions, promulgate regulations, exercise regulatory authority, and enforce actions and decisions, as directed by the Commission.

Executive-Driven Public-Private Partnership

FCSC Executives

The FCSC Commissioners will represent the perspectives of the FCSC in the executive partnership.

Private Sector Executives

Senior executives (CEO or immediately below) will represent their sector (energy, communications, or financial services) in the executive partnership.

Federal Senior Executives

Senior executives (S-1 or immediately below) will represent the departments, agencies, and regulatory bodies that have direct oversight of the affected sectors, plus principals from the Intelligence Community and law enforcement, in the executive partnership.

Leveraging the CICC to Counter Cyber Threats

While the FCSC as the ideal solution will take time to implement, the CICC can be stood up more quickly by leveraging existing authorities and with the support of the identified companies in the three sectors. As the FCSC is established, the CICC will continue to play a vital role. The steps below outline how the FCSC process could work in practice with the CICC.

1. **Major cyber threat to national security identified**: The Intelligence Community—through the collaboration in the CICC—identifies and evaluates threats to critical infrastructure. Private company experts provide valuable technical insights to federal partners regarding the implications of the threats for company operations and validate the threats for private industry. Company representatives also have access to their corporate cyber data and can provide real-time coordination and responses to federal representatives, providing a strong value proposition for both public and private partners. The CICC then produces intelligence products, in collaboration with public and private members, that are informed by private company information and technical input. Validated severe and/or urgent cyber threats to private infrastructure that, a) have the potential to impact national security, and b) are not being effectively mitigated through other means, are then presented to the Commission for potential regulatory action.
2. **Rapid assessment of cyber risk or issue**: Based on the CICC assessments, the Commission works with its staff and the CICC to make an initial determination if an action is required to address the cyber risk or compliance issue. Technical staff evaluate the potential impact and possible remedies. Policy staff review existing authorities to see if other departments or agencies can act to address the risk and determine if the mechanisms already exist to mitigate the threat (e.g., existing agencies). If not, the FCSC determines if it needs to provide directives to mitigate the threat.
3. **Consultation with Executive Public-Private Partnership**: The Commission staff brings their initial assessment to industry and government executives to obtain advice and guidance on proposed actions or remedies. The "three-party" partnership bodies engage expert staff and executives to gather analysis and recommendations for action.
4. **Commission decides on appropriate action**: The Commission makes a final determination on the needed actions to address the issue. This could result in a new rule, a referral to another agency or department with regulatory authority, or a proposed action that requires collaboration with other government entities and/or industry groups.

Core FCSC Functions

The table below describes how the FCSC would implement its core functions, and how near-term urgent actions will support FCSC implementation and be rolled into the FCSC as it is established.

Function	Urgent Action: Near-Term Recommendations	Comprehensive Solution: FCSC Implemented (Rec. 5)
Counter Severe Cyber Threats	• **Rec. 1:** Establish the Critical Infrastructure Command Center (CICC) • **Rec. 4**: Use the NLE 2020 to pilot the CICC	• Provide direction and technical resources to companies for rapid development and deployment of cyber mitigations • Exercise regulatory authority to direct private companies to take specific, enforceable mitigation actions to protect their cyber networks when threats, need for speed, or common direction are essential to meet important national security needs
Accelerate Information Sharing	• **Rec. 1**: Establish the CICC • **Rec. 2**: Prioritize detecting and identifying efforts to attack critical infrastructure • **Rec. 3**: Hold the TS/SCI briefing with the CEOs of identified companies	• Leverage the CICC to optimize bi-directional information sharing and accelerate mitigations • Identify ways to rapidly declassify information with broader sector and government implications and disseminate through existing effective channels (e.g., Information Sharing and Analysis Centers)
Ensure Supply Chain Integrity	• **Rec. 7**: Conduct a legal review of existing authorities that could be applied • **Rec. 9**: Continue and expand existing programs to independently test vendor equipment for vulnerabilities and report the results to private companies	• Set standards, rules, and/or regulations to ensure the security of equipment and services related to the IT and OT supply chain or affected companies. • Provide the regulatory authority to blacklist or whitelist components or services to mitigate severe cyber risks • **Rec. 8**: Liability protection to allow blacklisting and whitelisting of critical cyber products used in private critical infrastructure • Provide an independent evaluation of critical components using national laboratories of other resources

Function	Urgent Action: Near-Term Recommendations	Comprehensive Solution: FCSC Implemented (Rec. 5)
Provide Liability Protection	• **Rec. 7:** Conduct a legal review of existing authorities that could be applied	• Exercise existing or propose new regulatory authorities that limit the liability of private critical infrastructure companies that: o Share information with the government; o Take mitigation measures at the government's direction; or o Respond to the government's specific requests to take actions intended to protect, defend or restore critical cyber systems
Harmonize Regulations	• **Rec. 7**: Conduct a legal review of existing authorities that could be applied	• Serve as a cyber resource for federal agencies, provide cyber expertise and resources, and share insights into regulatory efforts • Identify conflicting and/or duplicative regulations across the federal regulatory framework and propose solutions
Share Best Practices	• **Rec. 6**: Convene a symposium (while the focus of the event will be on building out the FCSC and the path to implementation, part of the discussion will likely involve sharing experiences and knowledge)	• Coordinate with the Executive-Driven Public-Private Partnership to share best practices and mitigations used by targeted companies to increase protection and cyber hygiene across sectors

Operating Philosophy

- **The FCSC commissioners and industry and government executives will work collaboratively in the national interest**, through the "three-party" partnership, to set strategic direction, establish priorities, provide resources, and hold people accountable for results and outcomes. Moreover, the people engaged by the executives must have the authority to act on behalf of their organization, including quickly committing resources and personnel, with no (or minimal) prior approval.
- **Actions and decisions by the Commission must recognize the constraints of competitive market conditions and regulatory requirements** that critical infrastructure companies face, and they must provide solutions that enable the companies to act unimpeded by these constraints. This may include financial, regulatory, or policy remedies.
- **Bi-directional sharing of actionable classified information at the level needed is essential** and must occur with the speed and regularity needed to prompt private sector action. Focus should be on what needs to be done to mitigate the risk, rather than on sources and methods, to avoid the need for highly classified information from the TS/SCI space.
- **Prescriptive regulatory solutions to counter private sector risks should be avoided** unless: a) the private sector is not able to effectively and expeditiously act on its own; b) the government has unique technology solutions that are unavailable to the private sector to counter serious threats; or c) the government has classified information pertaining to impending nation-state threats that cannot be shared publicly. Any proposed regulatory framework should seek to establish the desired outcomes without dictating the specific solution.
- **Existing authorities, models, and capabilities should be leveraged**, where possible, to avoid duplication and accelerate practical solutions.

Appendix B. Acknowledgements

Working Group Members

J. Rich Baich, Chief Information Security Officer, AIG

William J. Fehrman, President and CEO, Berkshire Hathaway Energy

Richard H. Ledgett, Jr., Former Deputy Director, National Security Agency

Michael J. Wallace, Former Vice Chairman and COO, Constellation Energy

Working Group Support

Sam Chanoski, Director, Intelligence, Electricity Information Sharing and Analysis Center (E-ISAC), North American Electric Reliability Corporation (NERC); NIAC Point of Contact

Charles Durant, Director of National Security Policy and Resiliency Policy Adviser, Berkshire Hathaway Energy; NIAC Point of Contact

Gibson, Dunn, & Crutcher LLP, legal analysis

Work Session Participants

Mark Harvey, Senior Director, Resilience Policy, National Security Council (NSC)

Chris Krebs, Director, Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security (DHS)

Brian Harrell, Assistant Director, Infrastructure Security Division (ISD), CISA, DHS

Steve Harris, Deputy Assistant Director, ISD, CISA, DHS

Sue Armstrong, Associate Director, Strategy and Resources, ISD, CISA, DHS

Ed Canuel, Director, Critical Infrastructure Resilience, NSC

Sara Mroz, Director, Energy Policy, NSC

Working Group Interviewees

Keith Alexander, President and CEO, IronNet; former Commander, U.S. Cyber Command; and former Director, National Security Agency (NSA)

John C. "Chris" Inglis, Former Deputy Director, National Security Agency; Commissioner, Cyberspace Solarium Commission

Mark Montgomery, Executive Director, Cyberspace Solarium Commission

Department of Homeland Security Study Support Resources

Ginger Norris, Designated Federal Officer, NIAC

Jessica Eadie, NIAC Secretariat Support

Jim Carey, Nexight Group, LLC

Jack Eisenhauer, Nexight Group, LLC

Lindsay Kishter, Nexight Group, LLC

Beth Slaninka, Nexight Group, LLC

This study is dedicated to the tireless work of Jim Carey (November 13, 1951 – September 27, 2019), who supported the NIAC for more than a decade.

Appendix C. References

Coats, Daniel R. "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community." Before the Senate Select Committee on Intelligence. January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Commission on Enhancing National Cybersecurity (CENC). *Report on Securing and Growing the Digital Economy*. December 2016. https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

Das, Debak. "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know." *The Washington Post,* November 4, 2019. https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/.

Executive Office of the President. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (E.O. 13800)." May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

National Infrastructure Advisory Council (NIAC). *A Framework for Establishing Critical Infrastructure Resilience Goals.* 2010. https://www.dhs.gov/sites/default/files/publications/niac-framework-establishing-resilience-goals-final-report-10-19-10-508.pdf.

National Infrastructure Advisory Council (NIAC). *Clarifications on Executive Collaboration for the Nation's Strategic Infrastructure: Responses to National Security Council Questions.* 2015. https://www.dhs.gov/sites/default/files/publications/niac-ceo-report-response-nsc-final-12-01-15-508.pdf.

National Infrastructure Advisory Council (NIAC). *Convergence of Physical and Cyber Technologies and Related Security Management Challenges*. 2007. https://www.dhs.gov/sites/default/files/publications/niac-physical-cyber-final-report-01-16-07-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Partnership Strategic Assessment*. 2008. https://www.dhs.gov/sites/default/files/publications/niac-ci-partnership-assessment-final-report-10-14-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *Critical Infrastructure Resilience Final Report and Recommendations*. 2009. https://www.dhs.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Cross Sector Interdependencies and Risk Assessment Guidance*. 2004. https://www.dhs.gov/sites/default/files/publications/niac-interdependencies-risk-assess-transmittal-letter-02-26-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Evaluation and Enhancement of Information Sharing and Analysis*. 2004. https://www.dhs.gov/sites/default/files/publications/niac-eval-enhance-info-sharing-transmittal-letter-08-21-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Executive Collaboration for the Nation's Strategic Infrastructure*. 2015. https://www.dhs.gov/sites/default/files/publications/niac-executive-collaboration-final-report-508.pdf.

National Infrastructure Advisory Council (NIAC). *Framework for Dealing with Disasters and Related Interdependencies*. 2009. https://www.dhs.gov/sites/default/files/publications/niac-framework-dealing-disasters-final-report-07-14-09-508.pdf.

National Infrastructure Advisory Council (NIAC). *Future Focus Study: Strengthening the NIAC Study Process*. 2017. https://www.dhs.gov/sites/default/files/publications/niac-future-focus-study-strengthening-the-niac-study-process-final-508.PDF.

National Infrastructure Advisory Council (NIAC). *Hardening the Internet*. 2004. https://www.dhs.gov/sites/default/files/publications/niac-hardening-internet-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Implementation of EO 13636 and PPD-21.* 2013. https://www.dhs.gov/sites/default/files/publications/niac-eo-ppd-implem-final-report-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). *The Insider Threat to Critical Infrastructures*. 2008. https://www.dhs.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf.

National Infrastructure Advisory Council (NIAC). *Intelligence Information Sharing Report*. 2012. https://www.dhs.gov/sites/default/files/publications/niac-intel-info-sharing-final-report-01-10-12-508.pdf.

National Infrastructure Advisory Council (NIAC). *Optimization of Resources for Mitigating Infrastructure Disruptions.* 2010. https://www.dhs.gov/sites/default/files/publications/niac-optimization-resources-final-report-10-19-10-508.pdf.

National Infrastructure Advisory Council (NIAC). *Prioritizing Cyber Vulnerabilities*. 2004. https://www.dhs.gov/sites/default/files/publications/niac-cyber-vulnerabilties-final-report-10-12-04-508.pdf.

National Infrastructure Advisory Council (NIAC). *Public-Private Sector Intelligence Coordination*. 2006. https://www.dhs.gov/sites/default/files/publications/niac-intelligence-coordination-final-report-07-11-06-508.pdf.

National Infrastructure Advisory Council (NIAC). *Risk Management Approaches to Protection.* 2005. https://www.dhs.gov/sites/default/files/publications/niac-risk-management-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Sector Partnership Model Implementation*. 2005. https://www.dhs.gov/sites/default/files/publications/niac-sector-partnership-implem-final-report-10-11-05-508.pdf.

National Infrastructure Advisory Council (NIAC). *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*. 2017. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.

National Infrastructure Advisory Council (NIAC). *Strengthening Regional Resilience*. 2013. https://www.dhs.gov/sites/default/files/publications/niac-regional-resilience-final-report-11-21-13-508.pdf.

National Infrastructure Advisory Council (NIAC). *Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation*. 2018. https://www.dhs.gov/publication/niac-catastrophic-power-outage-study.

National Infrastructure Advisory Council (NIAC). *Vulnerability Disclosure Framework.* 2004. https://www.dhs.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf.

National Security Telecommunications Advisory Committee (NSTAC). *NSTAC Report to the President on a Cybersecurity Moonshot*. November 2018. https://www.dhs.gov/sites/default/files/publications/NSTAC_CyberMoonshotReport_508c.pdf/.

President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*. October 1997. https://www.hsdl.org/?abstract&did=986.

Sheth, Sonam. "Hackers breached a US nuclear power plant's network, and it could be a 'big danger.'" *Business Insider*, June 29, 2017. https://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6.

U.S. Government Accountability Office. "Nuclear Supply Chain: NNSA Should Notify Congress of its Recommendations to Improve the Enhanced Procurement Authority." August 8, 2019. https://www.gao.gov/assets/710/700794.pdf.

Walton, Robert. "First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say." *Utility Dive,* November 4, 2019. https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired*, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

CERTIFICATE OF SERVICE

I, Jim Erickson, hereby certify that I have this day served copies of the foregoing document on the attached lists of persons.

xx by depositing a true and correct copy thereof, properly enveloped with postage paid in the United States mail at Minneapolis, Minnesota

xx electronic filing

Docket No. E002/M-19-685

Dated this 17th day of January 2020

/s/

Jim Erickson
Regulatory Administrator

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
David	Aafedt	daafedt@winthrop.com	Winthrop & Weinstine, P.A.	Suite 3500, 225 South Sixth Street Minneapolis, MN 554024629	Electronic Service	No	OFF_SL_19-685_Official
Roxanne	Achman	rachman@co.benton.mn.us		531 Dewey Street Foley, MN 56329	Electronic Service	No	OFF_SL_19-685_Official
Christopher	Anderson	canderson@allete.com	Minnesota Power	30 W Superior St Duluth, MN 558022191	Electronic Service	No	OFF_SL_19-685_Official
Alison C	Archer	aarcher@misoenergy.org	MISO	2985 Ames Crossing Rd Eagan, MN 55121	Electronic Service	No	OFF_SL_19-685_Official
Ryan	Barlow	ryan.barlow@state.mn.us	Public Utilities Commission	121 7th Place East Suite 350 St. Paul, MN 55101214	Electronic Service	Yes	OFF_SL_19-685_Official
James J.	Bertrand	james.bertrand@stinson.com	STINSON LLP	50 S 6th St Ste 2600 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official
James	Canaday	james.canaday@ag.state.mn.us	Office of the Attorney General-RUD	Suite 1400 445 Minnesota St. St. Paul, MN 55101	Electronic Service	No	OFF_SL_19-685_Official
John	Coffman	john@johncoffman.net	AARP	871 Tuxedo Blvd. St, Louis, MO 63119-2044	Electronic Service	No	OFF_SL_19-685_Official
Generic Notice	Commerce Attorneys	commerce.attorneys@ag.state.mn.us	Office of the Attorney General-DOC	445 Minnesota Street Suite 1800 St. Paul, MN 55101	Electronic Service	Yes	OFF_SL_19-685_Official
Riley	Conlin	riley.conlin@stoel.com	Stoel Rives LLP	33 S. 6th Street Suite 4200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
George	Crocker	gwillc@nawo.org	North American Water Office	PO Box 174 Lake Elmo, MN 55042	Electronic Service	No	OFF_SL_19-685_Official
John	Farrell	jfarrell@ilsr.org	Institute for Local Self-Reliance	2720 E. 22nd St Institute for Local Self-Reliance Minneapolis, MN 55406	Electronic Service	No	OFF_SL_19-685_Official
Sharon	Ferguson	sharon.ferguson@state.mn.us	Department of Commerce	85 7th Place E Ste 280 Saint Paul, MN 551012198	Electronic Service	No	OFF_SL_19-685_Official
Edward	Garvey	edward.garvey@AESLconsulting.com	AESL Consulting	32 Lawton St Saint Paul, MN 55102-2617	Electronic Service	No	OFF_SL_19-685_Official
Janet	Gonzalez	Janet.gonzalez@state.mn.us	Public Utilities Commission	Suite 350 121 7th Place East St. Paul, MN 55101	Electronic Service	No	OFF_SL_19-685_Official
Michael	Hoppe	il23@mtn.org	Local Union 23, I.B.E.W.	932 Payne Avenue St. Paul, MN 55130	Electronic Service	No	OFF_SL_19-685_Official
Alan	Jenkins	aj@jenkinsatlaw.com	Jenkins at Law	2950 Yellowtail Ave. Marathon, FL 33050	Electronic Service	No	OFF_SL_19-685_Official
Linda	Jensen	linda.s.jensen@ag.state.mn.us	Office of the Attorney General-DOC	1800 BRM Tower 445 Minnesota Street St. Paul, MN 551012134	Electronic Service	No	OFF_SL_19-685_Official
Richard	Johnson	Rick.Johnson@lawmoss.com	Moss & Barnett	150 S. 5th Street Suite 1200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Sarah	Johnson Phillips	sarah.phillips@stoel.com	Stoel Rives LLP	33 South Sixth Street Suite 4200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official
Mark J.	Kaufman	mkaufman@ibewlocal949.org	IBEW Local Union 949	12908 Nicollet Avenue South Burnsville, MN 55337	Electronic Service	No	OFF_SL_19-685_Official
Thomas	Koehler	TGK@IBEW160.org	Local Union #160, IBEW	2909 Anthony Ln St Anthony Village, MN 55418-3238	Electronic Service	No	OFF_SL_19-685_Official
Michael	Krikava	mkrikava@taftlaw.com	TAFT Stettinius & Hollister, LLP	2200 IDS Center 80 S 8th St Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official
Douglas	Larson	dlarson@dakotaelectric.com	Dakota Electric Association	4300 220th St W Farmington, MN 55024	Electronic Service	No	OFF_SL_19-685_Official
Peder	Larson	plarson@larkinhoffman.com	Larkin Hoffman Daly & Lindgren, Ltd.	8300 Norman Center Drive Suite 1000 Bloomington, MN 55437	Electronic Service	No	OFF_SL_19-685_Official
Kavita	Maini	kmaini@wi.rr.com	KM Energy Consulting, LLC	961 N Lost Woods Rd Oconomowoc, WI 53066	Electronic Service	No	OFF_SL_19-685_Official
Pam	Marshall	pam@energycents.org	Energy CENTS Coalition	823 7th St E St. Paul, MN 55106	Electronic Service	No	OFF_SL_19-685_Official
Joseph	Meyer	joseph.meyer@ag.state.mn.us	Office of the Attorney General-RUD	Bremer Tower, Suite 1400 445 Minnesota Street St Paul, MN 55101-2131	Electronic Service	No	OFF_SL_19-685_Official
Stacy	Miller	stacy.miller@minneapolismn.gov	City of Minneapolis	350 S. 5th Street Room M 301 Minneapolis, MN 55415	Electronic Service	No	OFF_SL_19-685_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
David	Moeller	dmoeller@allete.com	Minnesota Power	30 W Superior St Duluth, MN 558022093	Electronic Service	No	OFF_SL_19-685_Official
Andrew	Moratzka	andrew.moratzka@stoel.com	Stoel Rives LLP	33 South Sixth St Ste 4200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official
David	Niles	david.niles@avantenergy.com	Minnesota Municipal Power Agency	220 South Sixth Street Suite 1300 Minneapolis, Minnesota 55402	Electronic Service	No	OFF_SL_19-685_Official
Carol A.	Overland	overland@legalectric.org	Legalectric - Overland Law Office	1110 West Avenue Red Wing, MN 55066	Electronic Service	No	OFF_SL_19-685_Official
Jeff	Oxley	jeff.oxley@state.mn.us	Office of Administrative Hearings	600 North Robert Street St. Paul, MN 55101	Electronic Service	No	OFF_SL_19-685_Official
Generic Notice	Residential Utilities Division	residential.utilities@ag.state.mn.us	Office of the Attorney General-RUD	1400 BRM Tower 445 Minnesota St St. Paul, MN 551012131	Electronic Service	Yes	OFF_SL_19-685_Official
Kevin	Reuther	kreuther@mncenter.org	MN Center for Environmental Advocacy	26 E Exchange St, Ste 206 St. Paul, MN 551011667	Electronic Service	No	OFF_SL_19-685_Official
Isabel	Ricker	ricker@fresh-energy.org	Fresh Energy	408 Saint Peter Street Suite 220 Saint Paul, MN 55102	Electronic Service	No	OFF_SL_19-685_Official
Richard	Savelkoul	rsavelkoul@martinsquires.com	Martin & Squires, P.A.	332 Minnesota Street Ste W2750 St. Paul, MN 55101	Electronic Service	No	OFF_SL_19-685_Official
Bria	Shea	bria.e.shea@xcelenergy.com	Xcel Energy	414 Nicollet Mall Minneapolis, MN 55401	Electronic Service	No	OFF_SL_19-685_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Ken	Smith	ken.smith@districtenergy.com	District Energy St. Paul Inc.	76 W Kellogg Blvd St. Paul, MN 55102	Electronic Service	No	OFF_SL_19-685_Official
Sky	Stanfield	stanfield@smwlaw.com	Shute, Mihaly & Weinberger	396 Hayes Street San Francisco, CA 94102	Electronic Service	No	OFF_SL_19-685_Official
Byron E.	Starns	byron.starns@stinson.com	STINSON LLP	50 S 6th St Ste 2600 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official
James M	Strommen	jstrommen@kennedy-graven.com	Kennedy & Graven, Chartered	200 S 6th St Ste 470 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official
Eric	Swanson	eswanson@winthrop.com	Winthrop & Weinstine	225 S 6th St Ste 3500 Capella Tower Minneapolis, MN 554024629	Electronic Service	No	OFF_SL_19-685_Official
Lynnette	Sweet	Regulatory.records@xcelenergy.com	Xcel Energy	414 Nicollet Mall FL 7 Minneapolis, MN 554011993	Electronic Service	No	OFF_SL_19-685_Official
Thomas	Tynes	jjazynka@energyfreedomcoalition.com	Energy Freedom Coalition of America	101 Constitution Ave NW Ste 525 East Washington, DC 20001	Electronic Service	No	OFF_SL_19-685_Official
Lisa	Veith	lisa.veith@ci.stpaul.mn.us	City of St. Paul	400 City Hall and Courthouse 15 West Kellogg Blvd. St. Paul, MN 55102	Electronic Service	No	OFF_SL_19-685_Official
Joseph	Windler	jwindler@winthrop.com	Winthrop & Weinstine	225 South Sixth Street, Suite 3500 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Yochi	Zakai	yzakai@smwlaw.com	SHUTE, MIHALY & WEINBERGER LLP	396 Hayes Street San Francisco, CA 94102	Electronic Service	No	OFF_SL_19-685_Official
Patrick	Zomer	Patrick.Zomer@lawmoss.com	Moss & Barnett a Professional Association	150 S. 5th Street, #1200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_19-685_Official