(Via cyberincentives@ntia.doc.gov)

April 29, 2013

Mr. Alfred Lee
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, D.C. 20230

Re: The National Rural Electric Cooperative Association Response to March 28, 2013 Notice of Inquiry of the U.S. Department of Commerce, National Telecommunications & Information Administration

Dear Mr. Lee:

The National Rural Electric Cooperative Association (NRECA) appreciates the opportunity to respond to the Notice of Inquiry issued by the National Telecommunications & Information Administration (NTIA) regarding what set of incentives would promote cybersecurity. Specifically, NRECA provides below its comments on the incentives that would promote participation in a voluntary program to be administered by the Department of Homeland Security to support the use by owners and operators of critical infrastructure and other interested entities of the Cybersecurity Framework being developed by the National Institute of Standards and Technology (NIST). NRECA believes its comments will highlight incentives that would be valuable to its members.

I. Background on NRECA

NRECA is dedicated to representing the national interests of cooperative electric utilities and the consumers they serve. NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent from non-NRECA members. The vast majority of NRECA members are not-for profit, consumer-owned cooperatives.

NRECA's members also include approximately 67 generation and transmission (G&T) cooperatives, which generate and transmit power to 668 of the 838 distribution cooperatives. The G&Ts are owned by the distribution cooperatives they serve. Remaining

distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives were formed to provide reliable electric service to their owner-members at the lowest reasonable cost.

It is also important to note that cooperative electric utilities represented by NRECA are small and not-for-profit entities. The size and legal organization of NRECA's members is an important factor in the comments made below. NRECA firmly believes that any incentives developed by the Federal government to assist with the implementation of the Cybersecurity Framework to be administered by the Department of Homeland Security (DHS) should be developed with the interest of consumer-owned and not-for-profit entities in mind, not just larger and for-profit entities. Thus incentives should also be developed that provide value to self-regulated entities such as cooperatives. Ultimately, this means that any cybersecurity incentives developed must not be a one-size-fits-all solution due to the many differences among electric utilities.

Lastly, we want to make sure that NIST and DHS are fully aware of the requirements and regulations that are already in place for the electric sector. These include the NERC cybersecurity standards and the Rural Utilities Service (RUS) Emergency Restoration Plan (ERP) regulations for RUS borrowers. Both of these require actions by electric sector entities that include enforcement of compliance with the NERC standards which are subject to monetary penalties for violations, and the compliance with the RUS regulations to ensure the continued ability to receive financing by RUS.

II. Proposed Incentives To Be Used In Conjunction with the NIST Cybersecurity Framework

Outlined below are a set of possible incentives that NRECA believes would encourage its members to make use of the Cybersecurity Framework currently under development by NIST. Again, NRECA provides comments on the following incentives in the context of encouraging small, not-for-profit entities to use the Cybersecurity Framework.

a. Information Sharing is a valuable tool for Cybersecurity Framework adoption

A critical component that would encourage greater adoption of the Cybersecurity Framework is information sharing. Particularly for smaller entities such as NRECA members, the sharing of critical threat information as well as best practices for responding to cyber threats would be an enticing method for encouraging adoption of the Cybersecurity Framework.

When discussing information sharing in this context, it is useful to define exactly the kind of information sharing that would be beneficial to NRECA members. As the Federal government is well aware, the volume of cyber risks and their extremely varied composition is - simply put - overwhelming. The risks and potential impacts are very different for public facing elements of a cooperative's internet-connected business systems (such as data security) and their industrial control systems that typically are not internet-connected or if they are, they are protected with more aggressive security schemes. Given that millions of attempted cyber attacks occur daily, it is effectively impossible for any one entity to identify and defeat such cyber risks, including threats and vulnerabilities. Instead, companies are naturally going to need to rely upon some assistance for governmental authorities, particularly in the form of helping to identify threats as well as threat trends.

In the context of the Cybersecurity Framework, effective information sharing will take the form of a timely and efficient mechanism to pass along threat data, warnings, and trend information to Framework participants. Examples of the kinds of information that would be useful to share would include signatures of known viruses and malware, known behavioral techniques of signatureless threats such as "Advanced Persistent Threats", information regarding potential vectors for introduction of cyber threats like counterfeit parts and software, and the sharing of best practices or policies to combat or defeat emerging threats and vulnerabilities. NRECA would suggest that the existing Defense Industrial Base information sharing pilot program be reviewed when considering whether to create a similar program outside of the Defense Department. That program has certainly enjoyed some successes, but there are certainly lessons to be learned there and a careful review of its effectiveness will be critical to ensuring that taxpayer funds are not spent on unnecessarily duplicative or marginally effective programs.

Inherent in this as well will be offering liability protections for the use of information shared under the Cybersecurity Framework. NRECA members are certainly strong advocates for the protection of personally identifiable information (PII), but at the same time they realize that there is a compelling need to share information that could accidentally include PII. The potential civil liability for the sharing of such information is a significant deterrent, and so NRECA encourages NIST, NTIA, DHS, and others to utilize existing mechanisms or develop alternate mechanisms that would protect Cybersecurity Framework adopters from such claims. NRECA also encourages the use of liability protection in the form of shields that protect an entity from claims that it should have acted upon information received under the Cybersecurity Framework, but did not. Even with the filtering that is likely to be performed by the government to help narrow the types of information shared to only the most useful, it is still likely to be a monumental task for NRECA members to determine what information is relevant and actionable. Accordingly, NRECA members should not have to be concerned that despite their best efforts to filter through the shared information, certain actions may or may not be taken that could lead to a cyber event. Only a liability shield offered as part of the Cybersecurity Framework (whether through the SAFETY Act or another mechanism) can resolve those concerns.

b. <u>Liability protections should be offered through the SAFETY Act</u>

As cybersecurity risks continue to increase, particularly with respect to the frequency and sophistication of the attacks, the possibility of litigation for damages caused by cyber events is seeing a parallel increase. NRECA members and others are increasingly concerned about such litigation, particularly given the inevitable difficulty and expense of defending such lawsuits. The fundamental problem is that fact finders will likely make their decisions based on whether the attacked entity had in place "reasonable" mitigation measures and response/recovery plans. The variability of what constitutes a "reasonable" measure or plan is immense, and therefore is practically unknowable. While industry standards in place and under development as well as the Cybersecurity Framework may help narrow the range of what is considered "reasonable", the unfortunate fact is that without an affirmative legal defense tied to a range of cybersecurity measures, potential adopters of any Framework will not be able to realize the full benefits of such a framework.

A mechanism for attaching affirmative legal defenses to the Framework is already in place and in use. DHS administers the Support Anti-Terrorism By Fostering Effective Technologies Act of

2002, or the "SAFETY Act". The SAFETY Act, which was passed into law as part of the Homeland Security Act of 2002 (the law authorizing the creation of DHS), is intended to offer affirmative legal defenses to companies that sell or otherwise deploy security technologies (which includes products, services, policies, and procedures) designed to deter, defeat, respond to, mitigate, or otherwise combat security threats. The SAFETY Act offers two types of liability protection. The first type of protection is known as "Designation", which sets a specific cap on damages that may be awarded in litigation following an attack, along with a prohibition on punitive damages and pre-judgment interest, as well as a requirement that SAFETY Act-related claims may only be brought in Federal courts. Under Designation, the cap on damages is equal to an amount of insurance that the "seller" of the SAFETY Act-approved technology or service must carry as a condition of the award.

The second layer of protection under the SAFETY Act is referred to as "Certification". A Certification award provides the same protections as a Designation, as well as a presumption of immunity from claims arising out of or related to the use of the SAFETY Act-approved technology or service. The protections of the SAFETY Act can be negated with a demonstration that the applicant committed fraud or willful misconduct in the submission of the SAFETY Act application to DHS.

One additional protection offered by the SAFETY Act is that only the "seller" of the approved technology or service for may be sued for claims arising out of or related to the attack. This means that companies that purchase SAFETY Act approved products and/or services, as well as any subcontractors, suppliers, or other entities that provide components to the "seller" are not proper defendants in post-attack litigation. Thus they may have their claims immediately dismissed.

Critical here too for Cybersecurity Framework incentive purposes is an understanding of when the protections of the SAFETY Act are triggered. As set forth in the SAFETY Act statute (6 USC § 441-444), the SAFETY Act applies to any unlawful act that causes harm to US persons, property, or interests (including economic interests) that uses or attempts to use instrumentalities, weapons or other methods designed or intended to injury or other loss to citizens or institutions of the United States. With that definition in mind it is clear that the SAFETY Act applies to cyber attacks, including those that cannot be tied to any one particular person, group, or motive.

There are multiple ways the SAFETY Act can be used to encourage the adoption of the Cybersecurity Framework. First, DHS can coordinate internally so that any time a company adopts the Framework, it will receive expedited consideration for SAFETY Act protections. Included within that would be a presumption that the Cybersecurity Framework is useful and effective against cyber attacks, and thus the company adopting it merits SAFETY Act protections for its adoption and implementation processes. Second, an element of the Cybersecurity Framework could be that companies using SAFETY Act approved cybersecurity technologies and procedures as part of their cyber protection plan would be an acceptable cybersecurity plan under the Framework. Third, when setting forth specific products and procedures to be followed, the Cybersecurity Framework would encourage companies to use SAFETY Act-approved products and procedures when implementing its Framework program.

In NRECA's view, the benefits of using the SAFETY Act as an incentive for adoption of the Cybersecurity Framework are obvious and many. First the SAFETY Act is already in existence

and performing admirably, thus allowing for the use of a readily implementable incentive. Second, the SAFETY Act provides tangible legal benefits and answers the difficult question for companies of what measures could be taken that would be considered reasonable in the event of litigation. Third, little to no additional Federal funds would need to be expended in order to adopt the SAFETY Act as a Cybersecurity Framework incentive. The SAFETY Act does not provide indemnification or reimbursement for losses, and further the structure of the DHS office administering the SAFETY Act is such that if it needed to be expanded, relatively few funds would be needed to do so.

Considering all of the above, the SAFETY Act is an excellent liability mitigation program that should be a core incentive offered as part of the Cybersecurity Framework. The SAFETY Act offers strong liability protections that will encourage entities to adopt the Cybersecurity Framework as it will provide *de jure* assurances that the measures undertaken are reasonable, thereby dissuading expensive, protracted, and unnecessary litigation post-cyber attack.

c. Expedited security clearances should be made available as part of the Cybersecurity Framework

Significantly related to the need for information sharing, as part of the Cybersecurity Framework, is the need for security clearances to be made available to private sector participants on an expedited basis. It stands to reason that much of the threat information being collected by the government is sensitive if not marked Secret or Top Secret. Without proper clearances, it will be difficult if not impossible for companies to receive and share information in a timely fashion.

Part of the challenge associated with cyber events is how rapidly they occur and how quickly they can change. Complex new viruses and malware can be developed in a matter of hours, and so companies do not have the luxury of an extended amount of time prepare themselves for possible attacks. Inherent within that is the need for information to be shared with the private sector quickly even if it is still classified as Secret or Top Secret by government officials. Without rapid sharing, the likelihood of a successful attack using a new or sophisticated virus or malware grows dramatically.

Therefore, an important incentive for the Cybersecurity Framework will be the need for participants to have select employees granted appropriate security clearances in an expedited manner. The granting of such clearances will help ensure that valuable information is passed along not only in a timely manner, but also in a way that is meaningful to end users such as NRECA members.

An additional note here is that as part of granting clearances, the Cybersecurity Framework incentive program should include the ability to expedite the granting of both Secret and Top Secret clearances. Clearly cyber threat information is going to be assigned different clearance levels, and those clearance levels should not be an unnecessary inhibitor in sharing the information with Cybersecurity Framework participants. Thus NRECA suggests that another positive will be an expedited process for granting clearances at any level for Cybersecurity Framework participants.

d. Encouraging the robust development of a cyber insurance marketplace.

One final incentive that should be tied to the Cybersecurity Framework is the integration of the risk management community into the Framework's development and implementation process. More specifically, insurance carriers and insurance brokers should play a role in the development of the Cybersecurity Framework and also should be directly educated by the government on the security value when a participant properly implements the Cybersecurity Framework.

By way of background, as the private sector has gained a better understanding of the potential losses associated with cyber events, so too has its interest in utilizing risk transfer mechanisms such as cyber insurance policies. Companies are increasingly seeking out insurance policies that will offer coverage for a cyber event, whether the result is loss of information or destruction of property. Industry is also struggling to seek insurance protection for intangible assets, such as intellectual property and trade secrets. It is difficult to obtain such coverage, however, as the valuation of those assets is difficult for insurance carriers to gauge much less underwrite an appropriate policy for the associated risk.

Further, similar to companies seeking to protect themselves from cyber attacks, insurance carriers and brokers also struggle with determining what will be effective and reasonable cybersecurity measures to implement. The confusion surrounding such security measures only makes the insurance underwriting process more difficult, and lends itself to insurance carriers limiting capacity (the total amount of cyber insurance available on a global basis) and being conservative with premiums and deductible limits. In other words, without having a good grasp on the risks, threats, and effective countermeasures, insurance carriers will be driven to taking conservative measures and keeping the cost of cyber insurance higher than it could otherwise be.

In order to address those issues, a positive incentive to be created as part of the Cybersecurity Framework would be the creation of a closer relationship with the insurance community in order to better explain the types of threats and vulnerabilities the Cybersecurity Framework is intended to counter, how it will work, and how proper implementation will measurably increase the cybersecurity posture of a company. If insurance brokers and carriers have this information, it will allow them to better price the risks associated with cyber losses, and provide more accurate and fulsome coverage to policyholders like NRECA members. In effect, a closer dialogue with the insurance industry will allow it to better understand how cybersecurity will be improved through the Cybersecurity Framework, and allow it to more confidently extend "good driver" discounts to Framework adoptees. This will be especially true if the Cybersecurity Framework is effectively tied to the SAFETY Act and its liability mitigation benefits.

Finally, as part of the Cybersecurity Framework, there should be engagement with the Department of Treasury and other entities to encourage coverage for cyber attacks under the Terrorism Reinsurance Program Reauthorization Act of 2007, or "TRIPRA". That program, which provides a federal backstop to insurance carriers in the event of a major terrorist attack, could well prove to be a valuable addition to the incentives associated with the Cybersecurity Framework. By making that insurance backstop also apply to cyber events, it will give greater comfort to the insurance carriers that a major cyber event will not cripple their companies.

III. Conclusion

NRECA appreciates the opportunity to express our views about what incentives can be tied to the Cybersecurity Framework, and how those incentives can encourage the use of the Cybersecurity Framework to materially improve cybersecurity. We look forward to continuing our government-industry partnership to achieve greater cybersecurity protections, and thank you for your efforts to identify incentives.

Please contact Laura Schepis, Senior Director, Legislative Affairs, at 703-907-5829 or laura.marshallschepis@nreca.coop or Barry Lawson, Associate Director, Power Delivery & Reliability, at 703-907-5781 or barry.lawson@nreca.coop if you have any follow-up questions about our comments.

Sincerely,

/x/

Laura Schepis
Senior Director, Legislative Affairs

Barry Lawson
Associate Director, Power Delivery & Reliability