Ascendant
Compliance Management

Partnering With You to Make Compliance a Source of Strength℠

194 Main Street
Salisbury, CT 06068
Tel. (860) 435-2255
Fax (860) 435-2264

546 Fifth Avenue, 18th Floor
New York, NY 10036
Tel. (212) 956-9142
Fax (212) 956-9782

3828 19th Street
San Francisco, CA 94114
Tel. (415) 640-7397

www.ascendantcompliance.com

February 9, 2016

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Views on the Framework for Improving Critical Infrastructure Cybersecurity
Response to NIST Request for Information (RFI)

1. **Describe your organization and its interest in the Framework.**

   Ascendant Compliance Management, Inc., located in Connecticut, New York and San Francisco, is a regulatory compliance and cybersecurity consulting firm which was founded in 2007 by founding partner and director Jacqueline Hallihan, who has over 25 years of operational and risk management experience.

   Ascendant Compliance Management employs a diverse range of consultants to serve our clients. Our experienced team includes attorneys, MBAs and professionals with many years of operational experience, as well as former chief compliance officers and regulators with the SEC and FINRA. Ascendant's strength rests in the breadth of our backgrounds and our commitment to provide practical solutions from a position of knowledge and experience about both regulatory compliance requirements and information security best practices.

   Ascendant is retained by hundreds of asset managers and broker-dealers in the U.S. and the U.K., including public companies and some of the world's largest institutional asset managers,

broker-dealers, investment consultants, pension consultants, wealth managers, and private equity and hedge fund managers. Offering over 200 years of combined experience, our team shares a philosophy and commitment to innovation, the highest quality client service, and educational training and technological solutions for diverse financial services companies worldwide.

Ascendant offers innovative regulatory compliance and cybersecurity consulting, assisting clients with implementation and ongoing evaluation of collaborative solutions. As partners with our clients, our goal is to provide a customized and dynamic program, one which allows them to focus on their core businesses and on the growth and operation of their services. Our mission is to assist firms in preserving their hard-won reputations by making cybersecurity and compliance sources of strength.

Ascendant prides itself on being ahead of the curve when it comes to identifying industry trends and assisting clients in developing regulatory and cybersecurity solutions to address risks before they end up on the radar of industry regulators. What sets Ascendant apart from our competition is our hands-on cybersecurity industry experience coupled with a solid understanding of the regulatory environment within which financial services firms operate, and our collaborative working relationship with these organizations.

Our experienced consultants stay abreast of cybersecurity trends and best practices through research, continuing education, attendance at industry leading conferences, and in-person discussions with SEC and FINRA staff (including examiners conducting cybersecurity examinations). In addition, due to our in-house expertise, our consultants are regularly requested to speak at regional and national conferences on compliance and cybersecurity topics, including those hosted by the National Society of Compliance Professionals (NSCP), the New England Broker/Dealer and Investment Adviser Association (NEBDIAA), and Schwab Compliance Technologies (SCT).

Ascendant's IT team holds numerous industry-leading cybersecurity certifications, including several which are among the limited certifications approved by the U.S. Department of Defense (DOD) for the performance of information assurance. Further, our cybersecurity certifications supplement the industry knowledge our IT consultants have obtained through hands-on experience as systems integrators, software architects and developers, and IT project managers.

Ascendant offers a comprehensive suite of cybersecurity services designed to proactively discover vulnerabilities and strengthen an organization's defenses. Those services include reviews of, and assistance with, development of customized cybersecurity policies and procedures, reviews of physical security controls and information security governance practices, network vulnerability scanning, and network penetration testing. Ascendant's on-site cybersecurity services include cybersecurity risk assessments and assistance with implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "Framework").

The following responses are informed by Ascendant's familiarity and experience in working with the Framework since its adoption two years ago, as well as Ascendant's prior experience and understanding of the various frameworks on which the NIST Framework is based – including COBIT5, which Ascendant's cybersecurity experts have used for many years. Our responses are further informed by Ascendant's risk assessment engagements at financial sector firms for nearly a decade, and through our cutting-edge implementation of the Framework in our Ascendant Compliance Manager (ACM) Software-as-a-Service (SaaS) risk management platform.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

Ascendant Compliance Management appreciates the opportunity to respond to this RFI as a subject matter expert, having consulted numerous financial services organizations on the assessment of enterprise information security risks since the inception of the firm. Since the issuance of Executive Order 1363 and the release of the initial version of the Framework on February 12, 2014, Ascendant has been able to leverage its cybersecurity consulting services to include assistance with implementation of the Framework by helping firms to assess their cybersecurity risks and subsequently map their policies, procedures and controls to a Current Profile and a viable Target Profile. Ascendant has represented, and continues to represent, multiple organizations in the financial services sector in implementing and using the Framework.

Ascendant has developed a proprietary Software-as-a-Service (SaaS) risk management application, the Ascendant Compliance Manager ("ACM"), which many financial services firms are using to manage their enterprise regulatory compliance and cybersecurity risks, including implementation of the Framework. Through its ACM application, Ascendant's clients are able to take advantage of the continuous improvement methodology and interact with their Framework implementation to track progress through a real-time interactive risk heat map which reflects changes in operational and business risk.

Ascendant's subject matter expertise has been developed over decades of consulting experience through its staff working with and understanding the business and operational drivers of organizations ranging from small firms to some of the largest ($100 billion+). Ascendant's in-house cybersecurity expertise includes undergraduate and graduate degrees in computer information systems, attorneys who have focused on information security and intellectual property, and staff who have taken and passed rigorous industry examinations including the Certified Information Systems Auditor (CISA®), Certified Information Security Manager (CISM®), and Certified in Risk and Information Systems Control (CRISC™) certifications from ISACA.

3. If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).

Ascendant uses the Framework in conjunction with its cybersecurity consulting services for financial sector firms. Ascendant meets with a firm's senior management to understand the firm's cybersecurity concerns, issues, culture and priorities. In addition, Ascendant reviews detailed cybersecurity documentation provided by a firm to assess the firm's readiness and

responsiveness to cybersecurity risks. Through a collaborative process, Ascendant works with a firm's senior management to map information security policies, procedures, controls, data flows, inventories and priorities to a Current Profile in each of the functions, categories and subcategories of the Framework. Where applicable, Ascendant assists the firm in developing a viable and reasonable Target Profile based upon a gap analysis with respect to regulatory and business requirements, budget, staff, resources and priority.

It has been Ascendant's experience that our financial sector clients use the completed Framework as both a risk management benchmark and as a communications tool. With respect to managing risk, Ascendant's clients have expressed (1) that the Framework helps them to gauge cybersecurity preparedness by analyzing the ability to respond to, and produce documents to evidence, each of the items in the Framework; and (2) that the Framework is useful as a communications tool for budget discussions with senior management, reporting to boards of directors, and in responding to due diligence requests from investors and clients.

4. What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?

Although it can be difficult to draw generalizations based upon the wide cross-section of financial services firms that Ascendant counts as clients, there are certain themes that have become discernible through our assistance with the implementation of the Framework.

Consistent with our understanding of the use of the Framework by other organizations, Ascendant's experience is that firms are utilizing the Framework Core along with the Current Profile and Target Profiles, but that the Implementation Tiers and Privacy Methodology are not as widely used. Where firms appear to be at the fullest Implementation Tier (Adaptive), we would generally indicate as such by noting that the firm has presently attained its Target Profile in light of current regulatory and business requirements and constraints.

It has also been our experience that some organizations, including Ascendant, have taken the opportunity to customize the Framework further through the addition of risk impact and likelihood metrics over time. Ascendant has developed a Risk Manager module within its ACM software solution to enable firms to evidence their implementation of any framework, including the NIST Framework for Improving Critical Infrastructure Cybersecurity, as well as to interactively visualize risk heat maps to chart changes over time – changes which can result from any number of factors including additional regulation, emerging cybersecurity threats, deployment of new technologies, and adoption of new policies, procedures and controls.

The growing success of Ascendant's Risk Manager module and overall ACM platform indicate that financial sector firms are searching for specific characteristics in risk management solutions; they must be understandable as an effective communications tool with senior management, cost-effective to implement, and able to serve as repositories for evidence of a cybersecurity gap analysis and to chart the implementation and monitoring of cybersecurity controls.

5. What portions of the Framework are most useful?

Ascendant has found the most useful portions of the Framework to be the Framework Core and Profiles, followed by the Informational References. Collectively, these components appear well-suited to enable firms to reasonably assess their cybersecurity posture over time and effectively communicate such posture in non-technical jargon to laypersons.

Within the Profiles, the Identify and Protect functions comprise the bulk of where we see most firms spending their time and efforts.

6. What portions of the Framework are least useful?

The Implementation Tiers do not appear to be as widely used as one might expect. However, given the present voluntary nature of the Framework, there appears to be no mandate that financial sector firms regulated by the SEC move their cybersecurity programs all the way to the Adaptive Tier; rather, current SEC requirements dictate that an organization's controls need only be "reasonably designed" – and not all firms will have the budget, staff or other resources to be fully adaptive in all subcategories.

Within the Profiles themselves, the least useful portion to date lies in the Respond and Recover functions. Those functions, while necessary and relevant, are quite redundant at the subcategory level and present perhaps the largest opportunity to expand and enhance the Framework.

Given that the Framework continues to be referenced by the SEC as part of its cybersecurity initiative and examination efforts, and further given the apparent one-to-one mapping between the Framework and the cybersecurity practices examined by the regulators of financial services firms, it appears that implementation of the Framework has, in essence, become the de facto standard of assessing the "reasonableness" of an organization's cybersecurity controls.

7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

Throughout 2014, Ascendant observed a growing awareness among financial sector firms of NIST and of the Framework itself. A number of early adopter firms and those striving for best practices gave way in 2015 to even wider acceptance of the importance of the Framework in managing cybersecurity risk.

Ascendant believes that financial sector firms are eager to implement the Framework as a means to document their cybersecurity risk management efforts and to assess areas warranting prioritization and improvement. However, use of the Framework could be increased with additional outreach by NIST – including through attendance at sector-specific industry conferences and facilitation of more information sharing on specific best practices and peer benchmarks.

8. **To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.**

   The Framework has helped reduce the cybersecurity risks of our clients by enabling them to obtain a comprehensive snapshot of their current state of affairs (and in some cases, of their lack of controls in certain areas) and to use this awareness to prioritize actionable steps to lower risk. The widespread adoption of the Framework across numerous sectors will likely continue to push late adopters to implement the Framework as well.

   Relevant metrics regarding the Framework itself include (1) an Implementation Percentage documenting the number of subcategories for which a firm has a response or solution relative to the total number of subcategories, (2) Implementation Duration, and (3) a Progress Indicator, or the number of items listed in a Target Profile which are ultimately achieved by a firm and moved into the Current Profile over time.

   As stated elsewhere in this RFI Response, additional relevant metrics are most likely those which have been customized by individual organizations, and include the interactive risk heat map in Ascendant's ACM software solution to track changes in current and target profiles over time while allowing documentation to be uploaded to support the changes in risk.

9. **What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?**

   The voluntary nature of the Framework, together with the inclusion of informational references built upon previously existing frameworks, suggests that the Framework presently is well suited to prevent duplication – since firms can voluntarily opt not to implement any portion of the Framework which would be redundant.

   However, the Framework is intended to be sector-neutral and technology-agnostic. Therefore, adherence to the Framework should be possible regardless of whether standards change or new regulations are adopted, unless such regulations require a different or specific framework or risk assessment process be used. Consequently, to prevent duplication, it appears necessary to permit the Framework to remain flexible enough for implementing firms to add to, delete from, or modify components as necessary to ensure compliance with applicable regulations and standards while still following its spirit.

   As a final point, it is important to note that there likely exists a juncture at which enough deletions have been made to the Framework by a firm that the New Framework cannot still be interpreted as following the spirit of the existing Framework. Additions to the Framework do not seem to present the same issue.

10. **Should the Framework be updated? Why or why not?**

    Ascendant believes that the Framework in its entirety should be reviewed no less than annually to determine opportunities for revision. While the Functions themselves are broadly designed,

comprehensive, and unlikely to change significantly, new technologies or cybersecurity threat vectors may emerge which could warrant additions or modifications to certain of the subcategories, even while maintaining the Framework's intent to remain technology-neutral. Furthermore, while the Framework contemplates that firms may add to the Informative References listed, an annual update of the Framework would provide an opportunity to incorporate new or revised Informative References as relevant and applicable.

11. What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

Ascendant's experience in working with the Framework has been in the context of assisting firms in the financial sector with performing a cybersecurity risk assessment and implementing the Framework, and more specifically within the financial sector, registered investment advisers and broker-dealers. Given that context, certain aspects of the Framework appear to be inapplicable to these types of firms. For example, subcategory ID.BE-1 (The organization's role in the supply chain is identified and communicated) is often confusing to investment advisers and broker-dealers, who do not generally view their services as constituting part of a supply chain. Ascendant believes that this subcategory should be removed in future iterations.

Although the Framework in intended to be a living document, we have found that firms are hesitant to leave any subcategories blank when implementing the Framework out of concern that a partial implementation is perhaps worse than not implementing the Framework at all.

In addition, PR.DS-7 (The development and testing environment(s) are separate from the production environment) is primarily applicable to investment advisers and broker-dealers who have proprietary development or who maintain their own applications or websites.

12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

Ascendant believes that the Informative References in the Framework are currently adequate.

13. Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?

The approach Ascendant uses in helping financial sector firms implement the Framework is to expand the Framework with additional data points including Risk and Likelihood classifications, and to maintain the data points in a database to chart changes in enterprise risk and implementation status over time. This facilitates the real-time generation of interactive heat maps which are useful communication tools for boards of directors, senior management and regulators. Incorporating into the Framework risk and likelihood classifications that firms can populate for each subcategory could certainly help other sectors or organizations not only in

managing their cybersecurity risks, but also in effectively communicating those risks to appropriate stakeholders.

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?

The NIST Roadmap contemplates several areas for inclusion in the Framework which Ascendant supports. Specifically, Item 4.1 (Authentication) and Item 4.7 (International Aspects, Impacts, and Alignment) appear ripe to inform the next iteration of the Framework. Dual-factor or multifactor authentication, if properly implemented, presents a cost-effective means to greatly improve upon the reliance of passwords alone for authentication. As data protection regulations evolve, particularly in Europe, it will be important to ensure that the Framework remains viable in balancing business needs and consumer privacy interests while striving for enhancements in cybersecurity posture.

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

The Framework is intended to be a living document. Therefore, a firm using a prior version of the Framework is not disrupted if the firm opts not to implement updates incorporated in future versions. However, it may also be necessary for stakeholders reviewing a firm's Framework implementation to readily ascertain the version of the Framework they are viewing. One option for introducing updates without unnecessary disruption is for Firms to include the version number of the Framework in their implementations, and to be permitted a one-year period of time from the formal release of an updated version to update their implementation of the Framework to the current version.

16. Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

The FAQs shared by NIST have been particularly helpful in communicating the use of the Framework in managing cybersecurity risk to firms interested in implementing the Framework.

17. What, if anything, is inhibiting the sharing of best practices?

Ascendant believes that several factors may be inhibiting the sharing of best practices, but that in many respects the problem lies in the fact that too much information on best practices may be inhibiting an understanding of them. There is an overwhelming amount of publicly available information on cybersecurity best practices, but the information tends to be laden with technology lingo and not written for the average layperson. Likewise, due to the quantity of information on best practices, it can be challenging for laypersons to identify the most relevant authoritative sources for best practices information.

In addition, in a competitive market there is often little incentive for firms to share their best practices with other firms and how they learned from past failures to implement best practices. It has been Ascendant's experience that sector-specific peer networking groups and industry conferences are the channels most conducive to productive sharing of best practices among firms. Questions which have arisen at Ascendant's national compliance and cybersecurity conferences have included "How did you implement policy X at your firm?" and "Which vendor did you use to implement control Y?"

18. What steps could the U.S. government take to increase sharing of best practices?

The U.S. government may be able to increase the sharing of best practices through incentives or through more public-private collaboration. The establishment of a vendor vetting and review process for the Framework may also enable the U.S. government to list relevant vendors and service providers offering solutions in each of the Framework subcategories, where applicable.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

An optional survey conducted annually may increase the likelihood of information sharing. Alternatively, a mandatory survey could be introduced, in which case it should be brief, concise, and not impose significant time or cost burdens on responding organizations. We recommend increasing participation in sector-specific information sharing forums such as FS-ISAC, but would require firms to provide information about cybersecurity practices if they also wish to be consumers of such information sharing.

20. What should be the private sector's involvement in the future governance of the Framework?

The private sector's involvement in the Framework should be limited to information sharing (in an anonymized manner) about use of the Framework. NIST should remain the governing body overseeing development of the Framework.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

NIST should remain the governing body overseeing development of the Framework. Please refer to response #20.

22. If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

N/A. NIST should remain the governing body overseeing development of the Framework. Please refer to response #20.

23. If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

N/A. NIST should remain the governing body overseeing development of the Framework. Please refer to response #20.

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

N/A. NIST should remain the governing body overseeing development of the Framework. Please refer to response #20.

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

N/A. NIST should remain the governing body overseeing development of the Framework. Please refer to response #20.

Respectfully,

Edward J. Yerzak

E. J. Yerzak, CISA, CISM, CRISC
Vice President of Technology
Ascendant Compliance Management, Inc.