National Institute of Standards and Technology Request for Information

"Views on the Framework for Improving Critical Infrastructure Cybersecurity"

The Boeing Company

9 February 2016

Table of Contents

Introduction

The Boeing Company is pleased to respond to the National Institute of Standards and Technology (NIST), addressing the questions contained in the RFI titled "Views on the Framework for Improving Critical Infrastructure Cybersecurity."

Boeing is the world's largest aerospace company and leading manufacturer of commercial jetliners and defense, space and security systems. Our success is based on providing our customers with state-of-the-art products based on our leadership in technology and innovation. Protection of the critical infrastructure and our own intellectual property that creates and sustains this technological leadership is at the core of our efforts and the key to future success.

Since the release of the Framework, we have done departmental and enterprise reviews of the company's cybersecurity programs and studied how they comply with the Framework recommendations. Our response is a composite view that represents our products from small UAVs, tactical and strategic weapon systems, fighters, bombers and weapons. It also represents our efforts to execute our security protocols in our information technology enterprise and engineer cybersecurity into our commercial aircraft. Finally, in our assessment of the Framework's implementation, we have addressed the questions most applicable to our experience and offer our suggestions for improvement from our best subject matter experts.

Boeing works tirelessly to defend its information, products and networks against attacks. We applaud the administration and particularly NIST's efforts to remain in constant dialogue with and for seeking improvements from the private sector to improve our nation's ability to defend, detect, and recover from cyber incidents.

Boeing's Support and Commitment

The Boeing Company is very pleased to support NIST's ongoing efforts to improve a cybersecurity framework. We are concerned both as an entity interested in protecting our own company, our products, the safety of the flying public and the aviation industry and as a contractor working on defense and cybersecurity for the federal government and other customers. We would like to reiterate several key points from our last submission:

- We believe that all stakeholders need to work together to share cyber threat information and best practices for prevention, detection, removal, and recovery from network attacks until a more secure information infrastructure can be developed and implemented.
- Boeing supports the establishment of standardized Government-Industry non-attributed, non-punitive Cyber Information Sharing forums that minimize the risk associated with self-reporting cyber threats, cyber-breaches and cyber-risk mitigation best practices with appropriate liability protection.

- Boeing supports voluntary cyber threat information sharing with government and private sector entities.

- Boeing supports the creation of industry-led cyber security best practices that result in straight-forward guidelines that ensure system critical infrastructure security, employ appropriate self-regulation by industry, and provide industry with liability protection similar to PL 85-804 and Anti-terrorism Technology (ATT) protections.

- Boeing supports efforts to facilitate industry's ability to manage the Insider threat, staying attuned to employee privacy and people risks.

- Boeing supports the creation of industry-led international cyber cooperation with processes and outcomes that are similar to, and not conflicting with, domestic efforts

Boeing is very pleased with the progress of cybersecurity legislation passed by the current Congress and signed by the administration. Programs like the NIST framework have proven to our lawmakers that the private sector approaches and best practices in cybersecurity are reliable, trustworthy, and operate effectively outside a government enforced compliance regime. Boeing is pleased to support ongoing efforts of NIST and further activities supporting this collaborative environment.

In summary, Boeing believes significant progress can be made if government and industry work together. The government should assist private sector efforts by providing incentives, assistance, and liability protections. Companies must be current with state-of-the-art defensive technology, nimble, innovative, and free from unnecessary regulatory interference or restrictions.

Thank you for the opportunity to respond to this strategic framework challenge. Boeing looks forward to working with NIST to address this very important issue.

Organization of the Responses to the RFI Questions

Our response to the NIST RFI is attached in the Excel worksheet per RFI instruction. It includes:

Section 1, "Use of the Framework" covers our organization and its interest in and experience with the Framework

Section 2, "Possible Framework Updates" covers our suggested changes

Section 3, "Sharing Information on Using the Framework" covers our experience with information sharing using the Framework

Section 4, "Private Sector Involvement in the Future Governance of the Framework"

Best practices, existing standards, and recommendations are listed in their appropriate subject matter area under this taxonomy and are so identified to aid NIST in compilation. These best practices are based on our extensive experience with managing the security services for a large, globally connected enterprise with hundreds of large customer

organizations and thousands of suppliers. Most of these represent actual implementations, some represent current projects and directions.

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	The Boeing Company is a Commercial Airplane, Defense Systems and Global Services Company. Boeing Commercial Aircraft develops, builds and sustains aerospace systems for domestic and international customers. Boeing Defense Systems develop, produce and support the DoD and IC with products and services in support of the warfighter, intelligence communities. Our interest is in the evolution of protections being applied to protect the US and Industries sensitive information and to the mission assurance of the products from cybersecurity threats. From a business perspective, the Framework provides a mechanism to evaluate and categorize risk. This is not only applicable to the business but also to the aviation industry and aerospace ecosystem. Boeing is in a unique position as the leading aerospace company to provide strategic direction and innovation from a cyber security perspective. Use of the Framework as a standard facilitates communication within the industry and allows for expeditious quantification and characterization of a cyber security event. Boeing both leverages the Framework for internal and industry collaboration efforts, and has been involved in the definition of the Framework to meet Aviation industry needs."	
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.	Framework User	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	The Boeing Company has found the framework useful in many ways. Boeing Defense Systems uses it for Cybersecurity primarily based on the application of the NIST Cybersecurity (CS) Framework derived by our DoD and IC customers. It appears through contractual obligations applied through the acquisition of products and services. This effort is as scoped through the acquisition and is applied regardless of the life cycle status or stage of the system. Boeing Commercial Airplanes uses the Framework as a reference model for our Aviation Information Security Protection efforts, and in tern uses the Framework as a reference model in coordinating with external aviation information sharing organizations (Aviation-ISAC, etc.), aviation standards development organizations (ARAC, ARINC, etc.), and aviation compliance organizations (FAA, DHS, TSA, EASA, JAA, CAA, etc.), while our IT Enterprise units uses it for a) Internal product cyber security risk evaluation and recommendations, internal executive communications, external cybersecurity assessment, external sales & marketing of cyber security services, external responses to RFIs and RFPs.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Boeing played a key role in the development of the NIST Cybersecurity Framework and Boeing Commercial Airplanes has utilized the Core and Implementation Tiers from the framework since 2013 as a means for assessing risk and identifying improvements needed for the Aviation Industry in a series of targeted Use Case studies and Tabletop Exercises. The Profile elements of the NIST Cybersecurity Framework that focuses on business needs has also been utilized to establish a new set of software development quality standards for the Aerospace Industry overall that will be implemented in 2016. Boeing Defense experience is one of applying NIST Framework to our products and services is primarily through CNSSP 22 Policy on Information Assurance Risk Management for National Security Systems. For the IT enterprise, the value of the Framework Core has been its ability to present a comprehensive approach to cybersecurity that reduces both gaps and duplications. Properly presented, the Framework Core has been a useful tool for communicating the importance of cybersecurity, initiating risk discussions, and evaluating overall cyber security preparedness. The Framework Core has been useful in providing context when discussing specific cybersecurity areas, programs or technologies. The Tiers have been useful in explaining risk management concepts, although with some limitations. For one organization, a baseline Profile, contrasted with a longer	
5	What portions of the Framework are most useful?	Boeing Commercial Airplanes has derived the greatest benefit from developing a holistic and integrated view of cyber security for its airplane products and business operations across each of the Core Functions and Categories from the NIST Cybersecurity (CS) Framework which encourages industry to cover all Identify, Detect, Protect, Respond, and Recover functions in its approach. Our Defense arm has found the Core is easiest to understand and explain. Tiers and Profiles a little less so. They are not directly applying the CS Framework but rather following the NIST RMF. The IT enterprise found Appendix A is the most useful section of the Framework. The concise definitions that are used to explain the Framework and the cited references increase the credibility of the document and are useful to locate additional information. These references should be reviewed on a periodic bases to ensure they continue to work as planned.	
6	What portions of the Framework are least useful?	There is confusion in the "Identify" function between actions that an organization can take to identify threats and the consideration of governance as part of identification. Governance might be better placed as an category and the associated subcategories under the Protection function. The respond and recover elements of the framework are very redundant. Not all of the categories fit for an OEM like Boeing regarding the maintenance of systems. The IT enterprise found The Risk Management section is great for explaining what to do but less helpful in explaining how to do it. For IT purposes, RMF is more applicable and as such the CS Framework is not directly applicable to our products and services. Aligning and directly applying to CS Framework would complicate the operational application of CS.	
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)?	Boeing Commercial Airplanes is using the framework to identify improvements needed for all elements of our business, including for Aviation Product Development. Since the Framework has been developed from a risk evaluation of an "as-is" enterprise perspective, the Framework does not provide a complete solution for supporting OEM product development and design of Future State ICS implementations. The AIAA Framework might be a place to look for additional elements to consider NIST Cybersecurity Framework modification.	
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.	Boeing Commercial Airplanes has already significantly reduced its airplane product, business operations, and manufacturing process cyber security risks through leverage of the NIST framework, including assessment of Implementation Tiers in development of process and functional technical improvement objectives for Boeing and its Airline Industry partners with the goal of achieving an Adaptive level of maturity for each of the framework functions. Our IT enterprise adds that the application of the concepts and principles defined in the Framework document has increased awareness of Cybersecurity issues and provided and approach to resolve these issues. The Framework in of itself may not have done much to reduce risk. It is the application of the principles that has reduced the 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?	It is recommended that the NIST Framework should focus on providing and supporting a global cross industry common set of definitions and a reference structure. Each critical infrastructure sector (IT, Finance, Power, Health Care, Aviation, etc.) will have unique regulatory requirements and standards needed to address the security implementation for that specific sector. Development of industry sector specific regulations and standards should be left to those industry sectors. This should include the appropriate government agencies associated with those industry sectors required to define and maintain the appropriate regulatory requirements and standards. For example, the commercial aviation sector has an extensive infrastructure already in place to address regulations and standards, including aviation information sharing organizations (DHS, Aviation-ISAC, etc.), aviation standards development organizations (ARAC, ARINC, ICAO, RTCA, etc.), and aviation compliance organizations (FAA, TSA, EASA, JAA, etc.). Boeing Defense adds that clarification of the relationship of CS to RMF would be helpful. Based on our contractual obligations we view RMF when it is applicable to our products and services. The role of CS and its apparent guidance to NIST RMF should be clarified. Our IT enterprise believes also that perhaps the most effective way to "prevent duplication" is to consolidate the cybersecurity effort within the government. Boeing has found that as organizations emphasize autonomy in addressing security that risk and vulnerabilities through inconsistent application of policy.	
10	Should the Framework be updated? Why or why not?	Yes, it should be updated to take into account initial experiences with it. Updates should be incremental, well planned and cautious or there is a risk of losing continuity and decreasing its value as a common communications mechanism. The Framework should be constantly monitored and updated to keep pace with the evolving global cyber technology and threat landscape.	

#	Question Text	Response Text	References
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.	The NIST Cybersecurity Framework provides a good functional model, but is not as cyclic as the NIST Risk Management Framework (2009) in providing a recurring process for risk management. Also the NIST Cybersecurity Framework does not cross reference and show integration with other NIST frameworks. Also, add Threat Intelligence as a Category under the Detect Function. It's not the same as event detection and, especially with the growth of ISACs, the NCCIC, etc., it needs its own area. The Respond and Recover Functions need some more filling out. Especially Recover, which is often not part of or well integrated with enterprise Cyber Security activities. Lastly, it really needs a more visible Governance section. Either a 6th Function or a Category under Identify. Too much of the governance (policies, RAA, etc.) are scattered in the Sub-Categories – which are not very visible. Some categories could benefit from additional information: (a) Most of the Identity Management domain is subsumed by a single subcategory, "PR.AC-1: Identities and credentials are managed for authorized devices and users." Since the Framework was released, these has been an increased focus on this area, so further definition would be beneficial. In particular, the concepts of identify vetting, strength of authentication including the number of factors used, identify federation, and confidentiality protection of the credential stores has become even more vital. This single subcategory is insufficient to address such a complex topic. (b) Software vulnerability management is inadequately described through ID.AM-2 (Software platforms and applications within the organization are inventoried), DE.CM-8 (Vulnerability scans are performed), and RS.MI-3 (Newly identified vulnerabilities are mitigated or documented as accepted risks). This is another area that has advanced significantly since 2013. Organizations often fail to: a. Include specific version numbers in their software inventories (in ID.AM-2), b. Use a comprehensive set of external vulnerability reporting data sources to complement the internal scans specified in DE.CM-8, and c. Confirm that the mitigations specified in RS.MI-3 were in fact successfully deployed (by a real-time check) and such data was fed back to update the software inventory in ID.AM-2 (c) Security within the System Development Lifecycle is not adequately addressed. It is not enough to simply say: PR.IP-2 (A System Development Life Cycle to manage systems is implemented).	
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?	The NIST Framework should consider product development and design in addition to just current functional framework elements. The CSF calls for risk management processes and the RMF (800-30/37) defines process but not terminology. The RMF Processes need to be combined with a formal taxonomy to help users break risk management into small enough pieces that they can handle. The OpenFAIR standard (taxonomy and definitions) is very useful for this. The use of a taxonomy also helps in explaining risk issues to executives and decision makers who are not cyber security specialists. Also, show how RMF satisfies CS. Map FIPS-199, FIPS-200, NIST 800-37, 39, 53A etc. to CS Framework steps. CS only maps to NIST 800-53, which is not a process but a catalog of controls.	
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?	Boeing Commercial Airplanes has started to use the Civil Air Navigation Service Organization risk assessment model, which utilizes the NIST Cybersecurity Framework to baseline and assess the improvements needed for risk reduction. There might also be an opportunity to look into what the respective Information Sharing and Analysts Centers ISAC (http://www.isaccouncil.org/) are doing from an implementation perspective. Also, www.safecode.org (of which Boeing is a member).	
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?	Boeing Commercial Airplanes utilizes the current and target Profiles as suggested to establish a roadmap for improvement under the NIST Framework to identify the level of improvement needed to become Tier 4 Adaptive in terms of cyber security. Our IT enterprise offers that all of these are valuable and all relate in some way to the Framework, but most are not evolutionary paths for the Framework, but rather complementary. Individual comments on each of these follow. (Numbered per the Framework Diagram) 4.1 Authentication – Valuable and necessary but only relevant to the Framework if it changed the taxonomy in the Framework Core. Divide Access Control (PR.AC) into Identification (PR.AC-1), Authentication (which is where IDESG, SP 800-67, and other authentication principles and artifacts would be collected), Authorization, Access Administration (essentially PR.AC-4) as well as Physical Access (PR.AC-2) and domain specific access (sort of a merger of PR.AC-3 and PR.AC-5). So, Authentication could become a sub category of Access Control. 4.2 Automated Indicator Sharing – This one is most relevant to the CSF itself. See comment 11 A above. If Threat Intelligence were a Category under Detect, this would be one Sub Category. 4.3 Conformity Assessment – Some discussion could be added to the risk management session at the beginning of the CSF document, but it would be better to have a separate document that guides organizations (such as ISACs or consortia) in the development of such criteria. Overall this needs to maintain the best practice approach of the CSF and give guidance to those organizations that want implementation indicators without becoming regulatory. 4.4 Cybersecurity Workforce – This should not affect the current CSF Core structure (PR.AT) 4.5 Data Analytics – While this is much broader than analyzing Threat Intelligence, some aspect of this certainly fits as a Sub Category of the proposed	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	The NIST Cybersecurity Framework only addresses the future specifically in terms of the "Recovery" improvements management function (RC.IM), but it does provide a solid framework for developing solutions around improvement for each of the NIST functions. The NIST framework descriptions should be modified to include future functionality. The framework should be a reference model. The instantiation of the Framework into an active business model creates the opportunity for disruption. The Framework needs to have a level/degree of separation from the operations of the business.	
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?	Formal meetings, conference presentations, and informal conversations with NIST, Intel and others have been very useful in providing guidance in using the Framework. While implementation details have somewhat intentionally been left vague so as not to prejudice or bias any specific implementation, examples are still very helpful in leveraging the Framework most efficiently. The development of the Civil Air Navigation Service Organization Security and Risk Assessment Guide (June 2014) has aided in Aviation Industry use of the NIST Framework by making practical recommendations for risk assessment derived from the framework.	
17	What, if anything, is inhibiting the sharing of best practices?	Critical Infrastructure industries and government partners vary in the maturity of their information sharing and discussion of best practices across industries. While many organizations have one to one relationships with other organizations, or supply chain relationships, scaling best practice information sharing requires some form of facilitation or overhead. I4 (International Information Integrity Institute) and ISF are two organizations that provide this as part of their member services. The ISACs are another great example. The formation of the Aviation ISAC has directly contributed to improvement in the sharing of best practices by Aviation Industry partners. However many organizations that could leverage these services do not want to pay the associated costs in time or money. Unfortunately, most organizations still do not understand the business case for or the importance of cyber security related information sharing. More mature organizations may feel that disclosing their best practices will give adversaries an edge that can be used against them. For example, as passwords have been replaced by PKI based two factor solutions, we have seen attacks shift towards those technologies. I4 and ISF counter this by enforcing member confidentiality clauses. An enterprise can generally avoid these types of attacks by sharing what their best practices are without sharing how they are implemented. Similarly, some enterprises may feel that their cyber security defenses are a	
18	What steps could the U.S. government take to increase sharing of best practices?	Continue support and coordination with the ISACs.	
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)?	The establishment of cross industry Use Case studies and Tabletop or other evaluation exercises would encourage organizations to share best practices and concerns over the use of the NIST Cybersecurity Framework from a practical implementation standpoint. Industry led consortia that are international in scope but also have healthy government participation is another thought. This mixture is the least threatening to enterprises and recognizes the global threat environment associated with Internet based commerce. However, parallel efforts should be tried and successful ones expanded.	
20	What should be the private sector's involvement in the future governance of the Framework?	Boeing recommends that NIST maintain the governance leadership roll for the Framework, at least for now. Private sector involvement could be solicited for Framework changes by leveraging the ISACs, where each ISAC might have one vote each on proposed changes to the Framework moving forward. The private sector should be the main contributor to any evolution of the Framework. The process for creating the original Framework worked very well, and far better than expected.	

#	Question Text	Response Text	References
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	For now, NIST should maintain leadership of the Framework, and the NIST Framework should be leveraged as a baseline reference by all industry standards organizations and utilized as a tool to enable consistency and improvements in implementation.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	If and when NIST might decide to transition governance of the Framework, the Framework should be transitioned consistently across each of the Core Functions, Profile levels, and Implementation Tiers	
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?	The ISAC community might provide for a future governance home for the Framework. Since the Framework is already becoming a Global International adopted Framework, recommend that eventually NIST transition the governance of the Framework to an appropriate international organization; potentially a United Nations affiliated organization.	
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?	Transitioning the Framework to a well established international standards body would support a minimally disruptive transition. Industry can better help in the transition once implementation tiers are assessed.	
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?	It would be beneficial for NIST to become better acquainted with international industry standards organizations working in this technology space, including the conformance and quality standards that are already in place for cross sector risk and security.	