CONCEPT PLUS

National Institute of Standards and Technology

Experience with the Framework for Improving Critical Infrastructure

Concept Plus RFI Response

Submittal Date: October 10, 2014

Submitted to:

National Institute of Standards and Technology
Diane Honeycutt
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899
cyberframework@nist.gov

Submitted by:

Concept Plus, LLC
12150 Monument Drive, Suite 615
Fairfax, VA 22033
Phone Number: 877-678-4660
Email Address: aabuzaakouk@conceptplusllc.com
Website: www.conceptplusllc.com

This includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed - in whole or in part - for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of --- or in connection with - the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data in this restriction is contained in the entirety of this proposal.

Concept Plus, LLC Points of Contact

Name:	Mr. Ahmad Abuzaakouk, President/CEO
Email Address:	aabuzaakouk@conceptplusllc.com
Phone Number:	703-436-8058
Fax Number:	888-450-7960
Level of Authority:	Authorized to hold discussions/negotiations with the Government and full authority to bind the company to a contract/order.

Name:	Mr. Rory Mclean, CTO, FSO, CISSP
Email Address:	rmclean@conceptplusllc.com
Phone Number:	703-436-8163
Fax Number:	888-450-7960
Level of Authority	Authorized to review any applicable performance evaluation reports rendered by the Government including electronic reports produced via CPARS.

Background:

The National Institute of Standards and Technology (NIST) requests information about the level of awareness throughout critical infrastructure organizations, and initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"). As directed by Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (the "Executive Order"), the Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Framework was released on February 12, 2014, after a year-long, open process involving private and public sector organizations, including extensive input and public comments.

About Concept Plus:

Concept Plus is a SDB and 8(a) certified consulting firm located in Northern Virginia. We combine our technical expertise with insights gained from our specific experience to provide effective and efficient solutions for our clients. We pride ourselves on being able to hire and retain highly trained and certified practitioners in Oracle, Cloud and Mobile technologies. Concept Plus has been appraised at CMMI Maturity Level 2 and our Agile Scrum Masters and ITIL trained staff ensure that our delivery and program management processes consistently follow industry best practices. Oracle Application Management, System Integration, Cloud Computing, and Mobile technologies are our core strengths, but superior client satisfaction is our core focus. To learn more, please visit www.conceptplusllc.com.

Our respondent, Mr. Rory McLean, CTO, FSO, CISSP has, for more than 20 years, specialized in developing and securing Oracle-based environments for both on-premise and cloud-based platforms. Having worked in both the Financial Industry and Defense Industry, Mr. McLean understands to necessity and the techniques for protecting highly sensitive information. In his role as CTO and FSO for Concept Plus, Mr. McLean has developed security solutions for numerous Federal agencies, including Department of Defense, Veterans Affairs, Securities and Exchange Commission, and Department of State.

For Further Information Contact:

Rory McLean, CTO, FSO, CISSP Work: 703-436-8163, Mobile 443-280-0781
rmclean@conceptplusllc.com

RFI Responses

Table 1: Questions for Industry - Current Awareness of the Cybersecurity Framework

#	Question	Response
1.	*What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?*	Concept Plus is a system integrator extensively working in both the DoD and Healthcare sectors. Within these sectors there is no clear impact of the Framework on the security operations taking place at a project or department level. The DoD sector issued a directive in March, 2014 that created a roadmap for converting from the old DIACAP approach to a NIST RMF (augmented by the CNSSI 1253 overlay). Adoption of the cybersecurity framework will not occur until this transformation is completed.
2.	*How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?*	As was suggested by several contributors in the commentary on the initial RFI, at the Program Office level security is exceedingly compliance minded whereas the framework is striving for better security rather than compliance. To be pushed down to the project level in the current culture, the CISO will need to make the Framework mandatory.
3.	*Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?*	As government contractors, our competitors seem to be more involved with the Framework than the government agencies we support. However, with agencies awarding projects to dozens of different system integrators, there is a robust ecosystem that could be tapped through information sharing. The agencies could serve as a central point for sharing information around attack vectors, risk modeling, and security controls.
4.	*Is there general awareness that the Framework:* *a. Is intended for voluntary use?* *b. Is intended as a cyber risk*	There is very little awareness of the Framework within our sectors.

#	Question	Response
	management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments? *c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?*	
5.	*What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework*	Given the compliance-minded approach to security, overt methods such as regulatory requirements is the fastest way to raise awareness and adoption. More covert methods such as networking, community of practices, or providing thought leadership on the topic will not improve adoption until the compliance minded attitude is changed.
6.	*Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?*	Does not apply to our organization
7.	*If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?*	Both DoD and Healthcare are government managed, and neither are promoting the Framework to any significant extent – at least, not at the program level. In the case of DoD, in March, 2014 they announced a major change in their system authorization approach by changing from DIACAP (DoD Information Assurance Certification and Accreditation Process) to a NIST RMF based approach (DoDi 8510.01). This directive enforces both the NIST RMF and additional overlays from CNSSI 1253. While the approach seems to be an effective way for a particular sector to customize the NIST RMF to the needs of a particular sector. It is more complex than the previous approach and

#	Question	Response
		requires re-education. As a result, these changes have not had any impacts at the Program Office level. We interact with the agencies at the program level. We see the Framework as more broad than the NIST RMF, addressing maturity levels (tiers) and profiles. If the Framework is being considered it is occurring above the Program Office level.
8.	*Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?*	To date we have authored whitepapers on security methodologies, held discussions with agencies on the topic, and we have included Framework concepts within in our responses to RFPs. While agencies have been receptive to these ideas, it doesn't appear they are aware of the Framework. The main issue is that the Program Office is taking a purely compliance view of security. To paraphrase one of the more cynical responses to our efforts, the Program Office's only concern is that security will not be a headache. The goal isn't the best security but the path of minimal effort to satisfy security obligations.
9.	*What more can and should be done to raise awareness?*	A culture of security rather than compliance is required. There are several approaches to changing this culture: ● The maturity model aspects of the Framework could be promoted the same way SEI provides CMMI assessments. A certifying organization that is a joint venture between government and industry could provide a security maturity assessment. This would not be a regulatory requirement, but simply a seal of approval like CMMI. ● Continue to promote concepts like continuous monitoring and resilience (over just hardening). The traditional approach to controls has created this "set and forget" approach to security. However, by focusing on resilience and continuous monitoring system owners will break from their "compliance" mindset and adopt a more security mindset.

Table 2: Questions for Industry - Experiences with the Cybersecurity Framework

#	Question	Response
1.	*Has the Framework helped organizations understand the importance of managing cyber risk?*	Internally, the Framework has helped solidify our organization's understanding of security strategy. The concept of tiers is used to measure our security capabilities on a maturity scale as we do with CMMi process. We have also adopted the "profile" concept by separating how we perform security vs. how we report security to the system owners. For example, in one particular case the agency only monitors 59 specific NIST controls. Internally, we still implement all the required controls and any additional controls and overlays that may apply. To satisfy the agency's compliance requirements, we define profiles that correspond to their compliance requirements…in this case, the 59 specific NIST controls. How we perform security is our "core" approach but how we report security to the system owner is a "profile".
2.	*Which sectors and organizations are actively planning to, or already are, using the Framework, and how?*	N/A
3.	*What benefits have been realized by early experiences with the Framework?*	N/A
4.	*What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?*	Concept Plus is a system integrator for both commercial and public customers. While security should be one of the highest concerns of the information owners, more often they are being dragged along via regulatory requirements. The Framework may be able to help change this culture by promoting a maturity model of an organization's security mechanisms. A maturity assessment will make it easier for Senior Management to assess their organization's readiness. As it stands, when an a noteworthy cyber attack occurs (such as Target or Home Depot) it is difficult for management to confirm that all the

#	Question	Response
		controls are in place, but they can understand if their organization is only tier 1.
5.	*Do organizations in some sectors require some type of sector specific guidance prior to use?*	The key term is "guidance". Taking the NIST 800-53 approach, security mechanisms can address organizational differences through additional the guidance. The controls themselves are more descriptive than prescriptive, but the guidance can make the control more prescriptive for certain sectors. An example of where this is already in place is with NIST guidance in support of FedRAMP requirements. For example, AC-01 leaves open the organization-defined frequency for reviewing account management policies, but FedRAMP dictates that anything less than annually is unacceptable. Similarly, the DoD is adopting the CNSSI 1253 overlays where applicable. A set of sector-specific guidances/overlays may dictate when the use of WiFi is unacceptable or dictate certain encryption algorithms or minimum encryption key lengths.
6.	*Have organizations that are using the Framework integrated it with their broader enterprise risk management program?*	Not at this time.
7.	*Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?*	The structure is very helpful, though we have restated the concepts into terms we are more familiar with: • "Tiers" have been equated with the CMMi. We are working on a roadmap on how to mature our risk management process and are planning on using many of the same processes we used during our CMMi assessment process. • "Core" aligns with the NIST RMF and is what we consider our security approach. • "Profile" is what we consider our approach to validating we are performing security correctly. To put this in the context of a government project, we strongly feel that the core should be how we conduct security operations, but the profile is the output we provided to the Program Office to validate our methodologies.

#	Question	Response
8. a.	*Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.* *a. Of these recommended practices, how are organizations initially using the Framework?*	Our use is largely #1 (*Basic Review of Cybersecurity Practices*). This is driven by having to satisfy other security obligations so the Framework is serving as a validity check against practices we have previously adopted. However, we are moving towards #2 (*Establishing or Improving a Cybersecurity Program*) as the Framework is enterprise-focused.
8.b.	*Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?*	Our organization is architecting a CAESAR-like monitoring system. Some of the Framework's high-level concepts and terminologies are factoring into our design. https://www.dhs.gov/xlibrary/assets/fns-caesars.pdf
8.c	*Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?*	As an organization that deals extensively with PII and HIPAA data, we address these concerns more directly than embedding controls in our security architecture. All employees receive annual training with periodic audit checks on how information is handled.
8.d.	*Are organizations changing their cybersecurity governance as a result of the Framework?*	There doesn't appear to be any significant changes in our sectors.

#	Question	Response
8.e.	*Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?*	Internally we are using aspects of the Framework to provide structure to our policies and strategies. Otherwise, there doesn't appear to be any significant changes in our sectors.
8.f.	Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?	*The Framework is not being presented as a "requirement" since it is not supported by corresponding legal obligations.*
9.	*Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?*	Sector leaders (such as DoD or HHS in our particular case) will need to push the standard down to the program level. However, it will need to be incorporated into the existing RMF to create a comprehensive, enterprise-level, and security architecture.
10.	*Have organizations developed practices to assist in use of the Framework?*	Not at this time.

Table 3: Roadmap for the Future of the Cybersecurity Framework

#	Question	Response
1.	*Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?*	Yes, of particular interest to our organization are 4.2 (automated indicator sharing) as it will help us develop a CAESAR-like monitoring tool. For this same reason we benefit from 4.5 (data analytics).
2.	*Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?*	Industry would benefit for a central repository of threat information which would help us identify attack vectors and develop risk models.
3.	*Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?*	No response