Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response

Cyber Security Framework Comments

The NRC has completed its review of the framework and provides the below comments in answer to the questions posed by NIST in the Request for Information (RFI) Notice.

Agency cyber security stakeholders and our critical infrastructure stakeholders are aware of the Framework. Many of the practices outlined in the framework serve as an active part of our corporate and critical infrastructure security programs. We plan to actively and periodically review our policies and cyber security practices against the final release of the Framework and we acknowledge the necessity and value it will provide to assist in updating our cyber security strategic planning, innovation and assessments as directed in Executive Order 13636.

We find the framework to be well articulated and we applaud the use of the Core Functions and Implementation Tiers as a way to best focus organizations on practices that lead to actionable and measurable results. We believe that the framework tenets should continue to be used on a voluntary basis, however, we note that regulatory entities should be empowered to leverage the Framework Core Functions as they deem essential to ensure that their entities establish and maintain meaningful and measurable programs to protect their critical infrastructures.

Framework Observations and Recommendations

Notwithstanding the publication of Special Publication 800-60, Revision 1, Guide to Mapping Types of Information and Information Systems to Security Categories, Volumes 1 & 2, gaps continue to exist between and across all organizations in implementing a common set of security controls to provide consistent protection, handling and processes of sensitive critical infrastructure and security-related information.

We recommend that the framework explicitly address or reference a set of concise and easily understood definitions and lexicons to enable an acceptable, baseline level of protection for all types of sensitive information.

The need for a reasonable and full treatment of sensitive information goes well beyond that of protecting civil liberties and privacy information. Protection of this information too, is important, but the framework should not stop at just these two sensitive information categories.

Our experience with various international, other Federal agencies, States, local law enforcement, cyber security auditors, and other agency stakeholders with whom we need to share information has oftentimes proven that each entity has its own definition of sensitive information and handles such information solely based on its own organization's risk level. While the NRC ensures that our licensees properly handle and process agency sensitive information through our issuance of NRC Cyber Security Regulations and agency governance, the lack of commonly accepted handling guidance negatively impacts our level of trust and limits the sharing of sensitive critical infrastructure information with those outside of the industries we regulate.

We recommend that NIST consider accelerating adoption of the Controlled Unclassified Information definitions and the minimum handling required to provide a common set of information protection requirements for all sensitive critical infrastructure information. We believe this to be essential in meeting the objective of the Cyber Security Framework's goal to improve the level of trust with regard to information sharing and cross collaboration across the critical infrastructure community.

Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response

Regarding the use of the Framework by NRC licensees, at this time the NIST Framework's application is not prevalent. In 2009 the NRC issued a mandatory new cyber security rule applicable to commercial power reactors. This new section of the NRC Code of Federal Regulations, Protection of Digital Computer and Communications Systems and Networks (10 CFR 73.54), requires existing nuclear power reactor licensees and applicants for new reactor licenses to submit a cyber security plan and an implementation schedule for NRC approval. The NRC has established a series of milestones for inspections involving identifying and protecting critical digital assets for power reactor licensees. As the NRC examines the need for cyber security requirements for other segments of the nuclear industry such as fuel cycle and spent fuel storage facilities, non-power reactors, decommissioned nuclear facilities, and materials licensees, the NIST Framework may be evaluated as a tool to achieve our objectives. We continue to work with other regulators to understand their successes and challenges with the Framework with particular interest in industry's acceptance and use of the NIST Framework.