NORTHROP GRUMMAN

Northrop Grumman Corporation

2980 Fairview Park Dr.
Falls Church, VA 22042

December 13, 2013

Adam Sedgewick
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899

Subject: Comments for the Preliminary Cybersecurity Framework, Executive Order 13636, Improving Critical Infrastructure Cybersecurity

Dear Mr. Sedgewick,

Northrop Grumman firmly believes that the voluntary National Institute of Standards and Technology (NIST) Cybersecurity Framework is a significant step in the right direction for providing assistance to critical infrastructure (CI) operators. Northrop Grumman commends NIST for working collaboratively to create a solid baseline Framework which, if adopted voluntarily by the critical infrastructure (CI) sectors and others, will help increase our Nation's collective posture and facilitate international cooperation in cybersecurity. Northrop Grumman appreciates NIST acknowledging the 1.0 Framework will continue to be developed as additional feedback and resources become available. Although the Framework is a good start, more needs to be accomplished to achieve the desired goals. This letter highlights some potential enhancements to the Framework.

Conformance Assessments: Implementation of the Framework should be measurable in order to provide incentives efficiently. Executive Order 13636 contemplates an incentive structure that would be created to entice entities to adopt the voluntary Cybersecurity Framework. Northrop Grumman understands the specific incentive structure is outside of the scope of NIST directives. However, if one is to incentivize an activity, it must be measured to ensure the proper rewards are applied. NIST has identified establishing measurable conformance criteria as an area for improvement for the Framework, noting "critical infrastructure's evolving implementation of Framework profiles should drive the identification of private sector conformity assessment activities." Northrop Grumman believes NIST should add additional measurable implementation criteria for each subcategory to create an initial baseline for conformance. Under the current Framework, two organizations in the same sector could self-assess a specific tier of maturity within the same profile, yet provide drastically different levels of security with substantially different costs. This level of ambiguity and variance in implementation potentially devalues the utility of the

Framework and could reduce adoption rates by not enabling cost-effective implementation. The Framework should provide repeatable assessments and objective comparisons. Strengthening baseline conformance assessments will enhance the benefits of Framework adoption.

Implementation Examples: The utility of the Framework would be increased for those critical infrastructure operators who might not be as mature in cybersecurity implementation if NIST would provide example implementations for each subcategory in the Framework. The Framework creates a common lexicon and standard with which to implement cybersecurity within the critical infrastructure sectors, but does not necessarily address examples of how the cybersecurity elements can be implemented. Absent more guidance, the Framework elements could be improperly estimated in terms of implementation costs, level of detail required, and overall impact of each element to the security posture of an organization. With such ambiguity, organizations could forego important security controls due to improper cost estimation, or expectations with respect to industry best practices. Implementation examples based on NIST's assessment of best practices could facilitate baseline implementation and thus increase successful adoption.

Software and Hardware Security: Best practices and standards to achieve software and hardware security, assurance, and quality should be added to the Framework. For example, CI operators could leverage the use of appropriate automated vulnerability analysis tools embedded in software code associated with Critical Digital Assets and/or Industrial Control Systems throughout their lifecycle. Software and System Assurance assessment and testing should also be integrated with Supply Chain Risk Management (Sec C.7). Northrop Grumman recommends NIST add Software and System Assurance as an area for future improvement. Inclusion of Software and System Assurance would align to the direction provided within the fiscal year 2013 National Defense Authorization Act (Sec. 933), which requires Department of Defense to address this area. Even though CI sectors may not be subject to any uniform requirements, it undeniably is a vulnerability that needs to be addressed by CI operators.

Framework Governance: It is not clear what the expected long term governance model for the Framework should be once the baseline is established. Since the Framework is so new, it seems plausible that the Government would maintain management of the Framework going forward with substantial Industry participation. However, some statements in the Framework suggest that the Government will divest itself of responsibility over the Framework and leave it purely to Industry. Clarification on the expectations of the Government with respect to long term governance of the Framework is necessary to properly set expectations.

Information Sharing: One area that could improve the practical utility of the framework and thus increase an adopter's security posture is including more explicit information sharing principles and guidelines. While the Framework does address the need for information sharing in a few areas, more guidance would be constructive,

specifically around the consumption of the information sharing activities developed under other sections of EO 13636. Many subcategories of the core have some element of information sharing either between organizations, between government and the organization, or between organizations and their stakeholders. Additional guidance on the implementation of information sharing standards, methods, content, and recommended limitations to sharing would help provide clarity on the issue, improve security postures, and facilitate inter-organizational and public-private information sharing efforts. Northrop Grumman believes information sharing is critical to successful cybersecurity, now and in the future, and this should be an explicit element of the Framework, particularly when addressed simultaneously with other core functions addressed in the Framework.

Northrop Grumman believes the NIST Cybersecurity Framework is a step in the right direction for improving our Nation's collective posture and facilitating international cooperation in cybersecurity. NIST has done a commendable job in synthesizing a holistic Framework with significant Industry participation. While this is a positive step, more needs to be done to continue to ensure our Nation's freedom and security in cyberspace. Northrop Grumman stands ready to assist NIST in further developing the Framework and facilitating its implementation.

Respectfully,

Dr. Michael Papay
Vice President and Chief Information Security Officer
Northrop Grumman Corporation