NORTHROP GRUMMAN

Northrop Grumman Information Systems

Cyber Solutions Division
15010 Conference Center Drive
Chantilly, VA 20151

April 8, 2013

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

Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Reference: National Institute of Standards and Technology Request for Information for Developing a Framework To Improve Critical Infrastructure Cybersecurity dated February 21, 2013 (“RFI) [Docket Number 130208119–3119–01]

Dear Ms. Honeycutt:

Northrop Grumman Systems Corporation, a Delaware corporation, acting through its Northrop Grumman Information Systems Sector, Cyber Solutions Division, is pleased to submit the enclosed written comments to the above referenced RFI to develop a framework for reducing cyber risks to critical infrastructure (the ‘‘Cybersecurity Framework’’ or ‘‘Framework’’). We appreciate this opportunity to collaborate with the National Institute of Standards and Technology (NIST), the United States Department of Commerce, other industry providers and industry-led standards bodies and look forward to supporting the NIST in its development of the Framework.

Northrop Grumman has identified certain cross-sector security standards and guidelines that we believe are immediately applicable or likely to be applicable to critical infrastructure as well as potential gaps in these existing standards and guidelines. As noted in its comments, Northrop Grumman believes the increased visibility and adoption of these standards and guidelines will help promote U.S. innovation and industrial competitiveness and help increase the national and economic security of the United States.

We believe that the standards and industry best practices that Northrop Grumman has identified will advance the objectives of the Executive Order 13636 and, where noted, are in line with voluntary international consensus-based standards. We also believe that, if incorporated into the Framework, they will provide a prioritized, flexible, scalable, repeatable, performance-based, and cost-effective approach to cybersecurity of critical infrastructure. They should also assist owners and operators of critical infrastructure and other interested entities in identifying, assessing, and managing cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties.

Northrop Grumman both knows and understands cybersecurity. Based on Northrop Grumman's extensive cybersecurity experience and its own deeply seeded mission objectives, we believe our comments in response to the RFI will provide the NIST with the necessary standards, guidelines, best practices, and possible frameworks for developing its own Framework to improve critical infrastructure cybersecurity throughout the critical infrastructure sectors of the United States.

Should you have any further questions that Northrop Grumman can answer, please direct your inquiries to Tim Reese, Program Manager, at (310) 795-0717 or by email to Tim.Reese@ngc.com; or, to Melissa Corbin, Contracts Manager, at (571) 313-2226 or by email to Melissa.Corbin@ngc.com. Again, Northrop Grumman appreciates this opportunity to support the National Institute of Standards and Technology in this important endeavor.

Respectfully,

Melissa A Corbin

Melissa A. Corbin
Contracts Manager

cc: Mike Papay (Northrop Grumman)
Brian Tulga (Northrop Grumman)
Tim Reese (Northrop Grumman)