April 5, 2013

VIA EMAIL TO *cyberframework@nist.gov*

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

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

Heartland Payment Systems, Inc. ("Heartland") respectfully submits to the National Institute of Standards and Technology ("NIST") this response letter to NIST's request for information ("RFI"), published in the *Federal Register* on February 26, 2013. NIST published the RFI in response to President Obama's February 12, 2013 Executive Order entitled "Improving Critical Infrastructure Cybersecurity" (the "Order"), which directs NIST to coordinate the development of a framework to reduce cyber risks to critical infrastructure. Through the RFI, NIST seeks public comment on existing cybersecurity standards which will fulfill the Order's directive to create a "flexible and repeatable" approach to "help owners and operators of critical infrastructure to manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties." The financial services standards NIST adopts in the cybersecurity framework will likely apply to Heartland, because it is one of the nation's largest payment processors, as well as a leading provider of payroll processing services, marketing solutions (including loyalty and gift cards), and school payment solutions.

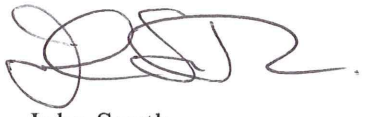
Heartland believes that NIST should include Special Publication 800-53 and the ISO 27000 series when creating cybersecurity standards for critical infrastructure in the payment processing industry. The positive attributes of these two existing standards would result in a flexible, yet structured, approach to financial services information security. Specifically, Special Publication 800-53, when combined with Federal Information Processing Standards 199 and 200, allows for the flexible adoption of standards based on: (a) the introspection of risks that are involved with each critical infrastructure entity's individual assets; and (b) how those risks intersect with that entity's security program. The ISO 27000 series, on the other hand, provides structure with baseline controls for implementing and maintaining information security management. The ISO 27000 series also includes a set of underlying standards designed to build and support a security program, such as auditing and management programs.

Adoption of a standard combining the ISO 27000 series and Special Publication 800-53 would be relatively easy for a broad spectrum of sectors, as many industries have already incorporated these existing standards into their information security programs.

Heartland further believes that there should be a standards development process specific to the financial services industry. The financial services industry is undergoing profound changes, as new technologies are created to meet consumer demands for innovative payment methods, such as mobile payment applications. These ongoing changes implicate specific technical issues not relevant to other industries and create unique challenges for the creation of an adoptable standard.

Thank you for your consideration and review of this letter. If you have any questions or wish to discuss this letter, please do not hesitate to contact any of the undersigned using the contact information provided below.

Respectfully submitted,



John South
Chief Security Officer
Heartland Payment Systems, Inc.
(972) 295-8800