STATE OF COLORADO

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

601 East 18th Avenue, Suite 250
Denver, Colorado 80203
Phone (303) 764-7700
Fax (303) 764-7725
www.colorado.gov/oit

John W. Hickenlooper
Governor

Kristin Russell
Secretary of Technology and
State Chief Information Officer

April 9, 2013

Diane Honeycutt
National Institute of Standards and Technology
Computer Security Division

Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

I am writing you to provide my professional feedback on the recently released Presidential Order titled "Improving Critical Infrastructure Cybersecurity," specifically pertaining to Section 7 subpart (a) and (b) regarding the development of a Cybersecurity Framework that provides "a prioritized, flexible, repeatable, performance-based, and cost-effective approach...to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."

For a brief background on myself, I currently serve as the Chief Information Security Officer (CISO) for the State of Colorado and have over a decade of cyber security experience, including within the military and private sector. I have worked in several roles, including as Colorado's Cyber Inspector General, a penetration tester, policy writer, software developer, cyber researcher, enterprise defender, and now as CISO. As the State's CISO, I am responsible for protecting between 30,000 – 50,000 endpoints and complying with all state and federal regulations and laws. When I first took on the State CISO job, I was required to drive down our risk profile with an operating budget of less than $10,000.

To sufficiently protect the state's systems and data with such a limited budget, I had to quickly identify and implement a cost-effective and proven cybersecurity framework. I made the decision to adopt and implement the "Critical Security Controls" (previously known as the SANS 20 Critical Controls), starting with the "First Five." I made this decision for the following reasons:

- **Offense must inform defense.** The controls are proven to prevent the majority of cyber attacks. As a person trained to "crack" into systems, I can confirm that the controls, starting with the "First Five," will prevent the majority of cyber attacks. This has been proven by the Australian national government and in my home state of Colorado.

- **The controls can be quickly implemented**. Colorado will implement the "First Five" controls across all state systems within 145 days.

- **The controls are cost-effective.** Colorado will implement the controls using a combination of open-source and commercial products at a cost of about $850,000 per year. This is a fraction of the cost required to comply with the myriad, overlapping, and non-prioritized federal regulations currently in existence.

- **The controls are prioritized and risk-based.** The controls are prioritized based on the amount of risk reduced by each control. With limited budgets, people, and time, this makes it easy to prioritize work and achieve the greatest return on investment for cybersecurity expenditures.

I would strongly urge you to adopt the Critical Security Controls as the baseline for developing the new Cybersecurity Framework. I believe the Critical Security Controls meet the Presidential Order's objective of creating "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" to cybersecurity.

I am available at your leisure to discuss the contents of this letter in more detail or to more directly assist in the development of the Cybersecurity Framework. I applaud the President and you on your efforts to improve the Nation's cybersecurity and am available to serve you in this effort as needed.

I can be reached via email at jonathan.trull@state.co.us or by phone at 303-949-5217.

Very Respectfully,

Jonathan C. Trull
Chief Information Security Officer
State of Colorado