From: Tim Lee <tim.lee@datacert.com>
Date: Thursday, April 4, 2013 4:15 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

I used to work at NASA's Johnson Space Center (JSC) managing the C&A (or now they call it A&A – Authorization and Accreditation) team for Engineering. We spent 500k annually on writing our SSPs and the center spent another 500K annually reviewing our SSPs and writing reports. We spent 1 million dollars annually on this paperwork exercise and if you were to ask Engineering if it knew where all their IT assets were, they would have no idea. Our SSPs were written to an asset inventory that we defined which rarely included all IT assets. The center/agency continues to let Engineers procure IT assets on credit cards which are then not reported as IT assets. The first step in securing an environment is to know what devices you have. Instead of spending a few dollars on fixing the process and requiring staff procurements using the defined PR process, we spent millions writing reports and tracking POA&M items. The agency uses RMS (developed by SecureInfo) as their central repository for SSP and POA&Ms. This system was designed to automate and streamline the audit process. It creates extra work for the operations folks who enter SSPs and POA&M items. It does not provided the tools the center needs to track POA&Ms so the center tracks it's POA&Ms in a separate database yet the agency still requires the use of RMS for reporting purposes. If implementation of the 20 critical controls where required instead of the SSP paperwork, NASA would be much more secure since they would be required to inventory their IT assets. Prioritization of resources would create an environment where dollars are spent wisely.

Tim Lee | Datacert, Inc.
IT Compliance Officer
Ph: 832.369.6098 | M: 281.236.3995