---------- Forwarded message ----------
From: **Matthew Santill** <msantill@broward.edu>
Date: Fri, Nov 1, 2013 at 10:51 AM
Subject: Preliminary Cybersecurity Framework Comments
To: "csfcomments@nist.gov" <csfcomments@nist.gov>

To whom it may concern,

I just had two comments on the Preliminary Cybersecurity Framework. I'm available for any assistance in designing this document. I think it looks great so far!

Broward College , while not technically housing any national security critical infrastructure, is one of the largest colleges in the nation with over 67,000 students.

Thanks,

Matthew Santill
Chief Information Security Officer | Broward College
Office: 954-201-7663 | msantill@broward.edu
Cypress Creek Administrative Center

6400 NW 6th Way

Fort Lauderdale, Fl. 33309

See Attachment.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	Broward College	Matt Santill, CISO		11	412	3.2	In the first stage the implementer will need to take inventory of critical systems as well as an inventory of where the electronic sensitive data resides in these systems. It is equally important that we note the physical locations of where information resides in both electronic and hard copy formats i.e. data centers, cabinets, offices, desks, closets. The framework should focus on hard copy information systems as well as electronic. We need to instill that the protection of PII is not just electronic. Having a shred bin readily available for employees is just as important as hard drive encryption. We would want an inventory of vendors and partners that may house critical infrastructure or information on our behalf. In later stages we will address controls around physical security of both hard copy and electronic sensitive information. We will also address proper vendor management controls.	Organization takes an inventory of critical information assets both in electronic and hard copy formats.