

**CS1/06-0174 IBM Contribution to CS1/06-0172: INCITS Working Draft:  
Confidential Information Security Standard**

1. § 6.1.8 and § 6.1.16 conflict. The later section only supports HTTP and HTTPS, whereas the first section supports additional secure protocols, e.g., SSH. I would think that the whole discussion w.r.t. allowed and disallowed ports should be more generic since good security policies arise from risk assessments and specific environments. For example, it might be an acceptable policy for an organization to allow FTP, as long as the data was encrypted before transfer and/or IPSec was always used to encrypt packets lower down in the stack.
2. § 6.2.4 -- IMO, WPA (and preferably, WPA2) should be the minimum level of WiFi security. At this date, no one should be using WEP.
3. § 6.3 -- Suggest adding a new subsection recommending "wipe on delete" (a.k.a. sanitation) for confidential information, with the system performance hit documented.
4. § 6.6 -- A general comment w.r.t. userids and passwords -- I recommend that use of passwords be discouraged. The Initiative for Open Authentication (OATH, <http://www.openauthentication.org>) is doing some good work in the area of strong authentication and provisioning.
5. General comment: I recommend inclusion of FIPS 199 and FIPS 200 as normative references.
6. General comment: It may be out of scope for this proposed standard, but do we want to include privacy-specific items w.r.t. confidential data? A subset of confidential data contains personally-identifiable information (PII) and/or HIPAA Protected Health Information (PHI). Privacy regulations (SOX, HIPAA, EU Directives, etc.) require more than standard CIA controls/countermeasures -- e.g., consent, purpose, reports.
7. General comment: Should we include higher-assurance mechanisms in addition to DAC and RBAC in this standard, for environments (per FIPS 199/200) that warrant it? This could include security labels, MAC, BLP information flow control, Biba integrity model, etc.