1. **Hardware Procurements**
   1. **Card Readers**. The Contractor (and/or any subcontractor) must include [Federal Information Processing Standard (FIPS) 201-compliant](https://www.idmanagement.gov/approved-products-list)) smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops.
   2. **Mobile Devices**. The contractor must follow NIST 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*and comply with Public Law 115-232 § 889*,* when purchasing mobile devices that process or store HHS/CMS data.
2. **Non-Commercial and Open Source Computer Software Procurements**

The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by the United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP) that will limit system software vulnerability exploits. The contractor will be liable for malicious or defective code or failure to reduce risk.

1. **Information Technology Application Design, Development, or Support**
   1. The Contractor (and/or any subcontractor) must ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.
   2. The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards, the Open Web Application Security Project (OWASP), and the *HHS Policy for Software Development Secure Coding Practices* that will limit system software vulnerability exploits.
   3. The Contractor (and/or any subcontractor) must ensure that computer software developed on behalf of HHS/CMS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor must test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS/CMS environment. No sensitive data must be used during software testing.
   4. The Contractor (and/or any subcontractor) must protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS/CMS must be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.
2. **Physical Access to Government Controlled Facilities**

"HHS reserves the right to exercise priorities and allocations authority with respect to this contract, to include rating this order in accordance with 45 CFR Part 101, Subpart A—Health Resources Priorities and Allocations System."