

ID	DCS SRD
DCS-118	Specific Requirements
DCS-119	Functional Requirements
DCS-120	Ingest Wideband Data
	The DCS shall have the ability to receive a single downlink contained within spacecraft
DCS-121	Acquisition of Signal (AOS) through Loss of Signal (LOS).
	The DCS shall terminate a capture if no data are received within 20 minutes of process
DCS-363	start-up, and no file shall be generated.
DCS-364	The DCS shall allow the operator to configure manual captures.
	The DCS shall be capable of ingesting Raw Computer Compatible (RCC) data in stacked
DCS-122	format from local and remote removable media playback device(s).
	During a live data capture from LGS, the DCS shall automatically suspend all other active
	functions and processes that do not pertain to wideband data capture or the Moving
DCS-123	Window Display (MWD).
DCS-124	The DCS shall make use of a contact schedule to automatically capture wideband data.
DCS-252	The DCS shall prevent the scheduling of conflicting missions on the same capture system.
DCS-167	The DCS shall allow operators to edit the contact schedule manually.
	The DCS shall be capable of ingesting Landsat 5 Wide Long-Term Multi-Satellite Archive
DCS-263	(WILMA) data in stacked format from removable media playback device(s).
	The DCS shall be capable of converting Landsat 5 Wide Long-Term Multi-Satellite Archive
DCS-264	(WILMA) data to Raw Computer Compatible (RCC) data.
	The DCS shall be capable of receiving Raw Computer Compatible (RCC) data from remote
	locations.
DCS-265	
	The DCS shall be capable of ingesting Landsat 5 TM Framed Raw Expanded Data (FRED) in
DCS-394	stacked format from removable media playback device(s).
	The DCS shall be capable of converting Landsat 5 TM Framed Raw Expanded Data (FRED)
DCS-395	to Raw Computer Compatible (RCC) data.
DCS-367	The DCS shall maintain capture-related specific information.
	The DCS shall be capable of capturing data independent of the database in contingency
DCS-368	situations.
	The DCS shall provide the ability to update the version field of raw files based on
DCS-369	predefined versioning options.
	The DCS shall verify that Cyclic Redundancy Checks (CRCs) are present in the associated
DCS-370	accounting files if the option is enabled.
DCS-125	Archive Wideband Data Files
DCS-126	The DCS shall facilitate the archive of all received wideband data files.
	The DCS shall be capable of stand-alone (native) archival of raw wideband data in a
DCS-127	stacked format to removable media.
	The DCS raw wideband data archive function shall be robust in nature, such that a failure
	of this function shall not inhibit a successful receipt, capture, and transfer of wideband
DCS-128	data to a processing system.
DCS-129	The DCS shall interface to archive systems for archiving raw wideband data.

DCS-131 The DCS shall automate the transfer of wideband data to tape media recording device(s).
DCS-132 The DCS shall track the status of the raw data transfer to the archive media and display the status on an operator Graphical User Interface (GUI).

DCS-133 The DCS shall identify all successfully archived wideband data for operator interpretation.

DCS-371 The DCS shall provide age checking of removable media to prevent overwriting new data. The DCS interface to archive systems shall serve as the primary path for a raw wideband data archive, and the DCS interface to removable tape media shall serve as the secondary (contingency) path for a raw wideband data archive.

DCS-134

DCS-135 Wideband Data Transfer

The DCS shall interface with a processing system for the electronic transfer of wideband data.

DCS-136

DCS-137 The DCS shall automate the transfer of wideband data to a processing system.

The DCS shall allow the operators to control the data transfer to archive and processing systems manually.

DCS-168

The DCS shall maintain and control operational parameters that specify where to transfer wideband data.

DCS-138

The DCS shall track the status of a wideband data transfer to a processing system and display the status on an operator GUI.

DCS-139

The DCS shall identify all successfully transferred wideband data for operator interpretation through an operator GUI.

DCS-140

The DCS shall have the ability to route data to a minimum of six multiple network-connected processing systems, under operator control, via an operator GUI.

DCS-141

The DCS shall maintain default transfer parameters for archive and processing systems specific to each Mission Id.

DCS-142

The DCS shall provide an automated clean up of stored wideband data files once the following functions are complete:

DCS-143

DCS-389 -Data capture.

DCS-390 -Data transfer to a processing system.

DCS-391 -Raw data archival.

The DCS shall allow for manual removal of captured data once the data capture is complete.

DCS-169

DCS-144 Operational Support

The DCS shall provide and maintain a log file of relevant operations, status, and health information for the operator.

DCS-145

DCS-146 Moving Window Display

The DCS shall provide a color MWD capability for the operator to view a reduced-size image of selected data bands extracted from the wideband data being captured.

DCS-147

DCS-173 The DCS GUI shall provide the ability to turn the MWD on or off.

DCS-243 The DCS MWD shall display the following:

DCS-149 -The Landsat video data.

DCS-151 -The spacecraft time code associated with the video data.

DCS-152 -The MODIS Bands 1-7 video data.

- DCS-374 -The next scheduled start time
The DCS MWD shall provide, but is not limited to, the following functionality during the data capture:
- DCS-153
- DCS-154 -The ability to switch the bands being displayed.
- DCS-155 -The ability to perform a dynamic contrast stretch.
- DCS-156 -The ability to scroll back to view previously displayed data.
- DCS-157 The DCS shall be capable of supporting multiple MWDs on one physical PC.
- DCS-158 The DCS shall allow for distributing the image data to multiple remote MWDs.
The DCS MWD shall be robust in nature such that a failure of this function shall not inhibit a successful receipt, capture, and transfer of wideband data to a processing system or an archiving system.
- DCS-159
- DCS-248 The DCS MWD shall allow, but is not limited to the following functionality:
- DCS-249 -The ability to configure the region to be selected.
- DCS-251 -The ability to choose between the full-resolution MWD or the subsampled MWD.
- DCS-160 Production
- DCS-161 Monitor and Control
- DCS-162 The DCS shall supply a GUI.
- DCS-163 The DCS GUI shall display, but is not limited to, the following:
-The name of captured wideband data files (a file is defined as a continuous stream of computer-compatible data).
- DCS-164
-File status (capture status, processing system transfer status, and raw archive transfer status).
- DCS-165
- DCS-375 -Color coding based on Mission Id
- DCS-376 The DCS shall automatically initialize at startup all capture systems as configured.
The DCS GUI shall allow the adding and deleting of conflicting missions based on the Mission Id.
- DCS-377
The DCS GUI shall allow the operator to initiate and stop manual raw data captures on any capture system.
- DCS-378
The DCS GUI shall provide a method to delete a file as an option when stopping a manual capture.
- DCS-379
- DCS-170 The DCS shall allow for manual configuration of the DCS tape device(s).
- DCS-171 The DCS shall allow the operator to suspend automated clean-up functions.
- DCS-172 The DCS GUI shall allow operators to configure an MWD.
- DCS-272 The DCS shall allow the operators to define a priority for each mission.
The DCS GUI shall allow the operator to close any editable window without saving the changes.
- DCS-380
- DCS-381 The DCS shall monitor local and remote disk usage.
- DCS-174 External Interface Requirements
- DCS-382 MOC
The DCS shall receive mission contact schedules delivered from each Mission Operations Center (MOC).
- DCS-383
The DCS shall have the ability to poll the schedules directory for new contact schedules and automatically ingest the received schedule files.
- DCS-384
The DCS interface with the MOC shall follow the Interface Control Document (ICD) between the MOC and the Ground Segment.
- DCS-385

- DCS-175 LGS
The DCS shall interface with LGS to receive bit synchronized Raw Computer Compatible (RCC) data at a Bit Error Rate (BER) no greater than 10⁻⁸.
- DCS-176 The DCS shall receive and store computer compatible bit data streams electronically from LGS, as documented in the LGS to DCS ICD.
- DCS-177
- DCS-178 The DCS shall be capable of sending raw data as well as test data, either generated by the DCS or received from the LGS Bit Error Rate Tester (BERT), to the LGS.
- DCS-179 The DCS interface with the LGS shall follow the ICD between the DCS and the LGS.
- DCS-180 LAM
- DCS-181 The DCS interface with the LAM shall follow the ICD between the DCS and the LAM.
- DCS-182 LACS
- DCS-183 The DCS interface with the LACS shall follow the ICD between the DCS and the LACS.
- DCS-184 MODIS
The DCS interface with the MODIS Processing System (MPS) shall follow the ICD between the DCS and the MPS.
- DCS-185
- DCS-186 LPS
- DCS-187 The DCS interface with the LPS shall follow the ICD between the DCS and the LPS.
- DCS-188 User Interfaces
- DCS-189 Hardware Interfaces
- DCS-190 Software Interfaces
- DCS-191 Communications Interfaces
- DCS-192 Performance Requirements
- DCS-193 The DCS shall receive and store computer compatible data as listed below:
-Landsat 7: A minimum of 75 Mbps for each channel for a minimum aggregate receive capability of 150 Mbps for a dual channel stream.
- DCS-194
- DCS-195 -Landsat 5: A minimum of 85 Mbps for the single channel stream.
- DCS-196 -EO-1: A minimum of 105 Mbps for the single channel stream.
- DCS-197 -Terra MODIS: A minimum of 13.1 Mbps for the single channel stream.
- DCS-198 -Aqua MODIS: A minimum of 15 Mbps for the single channel stream.
- DCS-199 The DCS storage device(s) shall support the following data transfer rates:
-Landsat 7: A minimum of 75 Mbps for each channel for a minimum aggregate receive capability of 150 Mbps for a dual channel stream.
- DCS-200
- DCS-201 -Landsat 5: A minimum of 85 Mbps for the single channel stream.
- DCS-202 -EO-1: A minimum of 105 Mbps for the single channel stream.
- DCS-203 -Terra MODIS: A minimum of 13.1 Mbps for the single channel stream.
- DCS-204 -Aqua MODIS: A minimum of 15 Mbps for the single channel stream.
- DCS-386 The DCS GUI shall take no longer than five seconds to display a selected GUI.
- DCS-205 Design Constraints
- DCS-206 Standards Compliance
The filenames created by the DCS shall conform to the Raw Computer Compatible (RCC) Data Format Control Book (DFCB).
- DCS-207

- DCS-387 The DCS shall comply with the Landsat Metadata Description Document (LMDD).
- DCS-208 Hardware Limitations
The DCS shall adhere to CTS and DDS System Build and Configuration Guide hardware specifications.
- DCS-388 The DCS shall make use of Linux operating system platform(s) that will support Myriad high-speed serial interface technology to receive Raw Computer Compatible (RCC) data accurately.
- DCS-224 The DCS architecture shall not preclude the insertion of a second Myriad high-speed serial interface card for either hot sparing or capturing of additional data streams (subject to the limitations of the attached wideband data storage transfer rates).
- DCS-225 The DCS storage device(s) shall ensure the integrity and continuity of captured wideband data.
- DCS-226 The DCS shall make use of standard network interfaces to transfer wideband data to a processing system.
- DCS-227 The DCS shall not require the presence of a Myriad high-speed serial interface card in order to ingest Raw Computer Compatible (RCC) data in stacked format from local and remote removable media playback device(s).
- DCS-228
- DCS-229 The DCS shall be capable of storing a minimum of 144 GB of unique wideband data.
- DCS-215 Attributes
- DCS-216 Availability
The DCS shall provide the capability to support operations 24 hours per day, 7 days per week, on a continuous basis.
- DCS-273
- DCS-217 Security
The DCS shall conform to SEC-101 Landsat Program Security Policy: Privileged Account Access and Maintenance of the Landsat Network.
- DCS-278
- DCS-279 Unix System Access Guidelines
The DCS shall ensure that the System Administrator does not have access to the Unix system 'root' account by logging on remotely as the root user.
- DCS-280 The DCS shall allow direct access to the Unix system 'root' account only from the system console.
- DCS-281
- DCS-282 The DCS shall note in the system log each direct privilege account access (root login).
- DCS-283 The DCS shall record in the system log who used the direct privilege account.
The DCS shall record in the system log the timeframe that the Unix system 'root' account was active.
- DCS-284 The DCS shall allow the System Administrator remote access to the root account to log on the system under their individual account name and password and then be able to su to the 'root' account.
- DCS-285
- DCS-287 Password Guidelines
- DCS-288 The DCS shall ensure that root account passwords will be unique from other Projects.
The DCS shall ensure that System Administrator account passwords will be unique from other Projects.
- DCS-291

- DCS-292 The DCS shall ensure that all passwords are at least eight characters in length with a minimum of two alpha and two numeric characters.
- DCS-293 Privileged Account Access
- DCS-294 The DCS shall support a System Administrator who shall be as restrictive as possible by using the least privileged approach to grant access to system users.
- DCS-295 The DCS shall support a System Administrator who shall ensure password conformance through periodic system access checks.
- DCS-300 Landsat Machine Setup Procedures: Networking
- DCS-301 The DCS shall ensure routing broadcasts are disabled.
- DCS-302 The DCS shall ensure ipforwarding in the kernel is disabled.
- DCS-303 The DCS shall ensure gated, mouted, and routed are turned off.
- DCS-304 The DCS shall ensure timed (time daemon or Time Synchronization Protocol (TSP)) is disabled.
- DCS-305 The DCS shall ensure timed (time daemon or Time Synchronization Protocol (TSP)) is replaced with NTP (Network Time Protocol).
- DCS-306 The DCS shall conform to SEC-102 Landsat Program Security Policy: Installation and Use of a Secure Shell Environment on the Landsat Systems.
- DCS-308 Secure Shell Environment
- DCS-309 Installation of a Secure Shell Environment
- DCS-317 The DCS shall be configured with a secure shell application.
- DCS-318 The DCS shall be configured with the latest version of the secure shell application available for download, unless incompatible.
- DCS-319 The DCS shall use a secure shell application compatible with other secure shell applications at EROS.
- DCS-320 The DCS shall use renamed factory-supplied secure shell executables to avoid unintentional usage.
- DCS-321 The DCS shall have secure shell access rights to 000 to prevent any access except by root.
- DCS-322 The DCS shall use links between the secure shell command and the old executable.
- DCS-314 Use of a Secure Shell Environment
- DCS-323 The DCS shall prevent all users from being able to execute the factory-supplied executables for telnet, rlogin, rsh, and rcp.
- DCS-324 The DCS shall use the secure shell-computing environment whenever possible.
- DCS-325 The DCS shall permit continued secure access between two hosts once a trusted relationship is setup.
- DCS-326 The DCS shall conform to SEC-103 Landsat Program Security Policy: Use of X Access and Control.
- DCS-315 X Access Control: X Window Session
- DCS-327 The DCS shall use a secure shell environment as the preferred method for gaining and controlling access to an X window.
- DCS-328 The DCS shall use secure shell to tunnel the necessary X protocol, automatically and transparently, to the connected system to maintain a secure X environment.
- DCS-316 X Access Control: Xauth Function
- DCS-331 The DCS shall use Xauth authentication as the preferred method to control the X environment to the user.

- DCS-329 X Access Control: Xhost Function
- DCS-332 The DCS shall use Xhost on a limited basis for a server-based access control mechanism.
- DCS-333 The DCS shall avoid using the Xhost + configuration.
The DCS shall conform to SEC-135 Landsat System Security Plan: Major Application
- DCS-334 Security Plan.
- DCS-330 Identification and Authentication
- DCS-341 The DCS shall ensure passwords have a minimum of eight characters.
- DCS-342 The DCS shall ensure passwords are changed every 90 days.
- DCS-343 The DCS shall use the root account as a group account in UNIX-based systems.
The DCS shall ensure system users change the password after the first login upon creation
- DCS-344 of a new account.
- DCS-335 Logical Access Controls
- DCS-345 The DCS shall limit access for operations group accounts to necessary parts of the system.
The DCS shall place departmental or bureau-approved warning banners on login screens
- DCS-346 and FTP access.
- DCS-336 Public Access Controls
- DCS-347 The DCS shall limit access controls to what the user can read, write, modify, or delete.
The DCS shall use controls to prevent public users from modifying information on the
- DCS-348 system.
- DCS-337 Audit Trails
- DCS-349 The DCS shall use system activity logs to trace user actions.
- DCS-350 The DCS shall use operations logs for system activities and problems encountered.
- DCS-351 The DCS shall use system performance logs and statistics.
The DCS shall not write passwords to log files, system process descriptions (ps
- DCS-352 commands), or echo passwords to the terminal when entered.
- DCS-218 Maintainability
- DCS-354 The DCS shall provide the capability to isolate system faults.
- DCS-355 The DCS shall provide the capability to recover from system faults.
The DCS shall permit corrective maintenance to be performed on failed equipment while
- DCS-356 the remainder of the system is actively satisfying mission-critical functions not supported
- DCS-357 by that equipment.
The DCS shall provide the capability to test DCS functions and external interfaces in an
- DCS-357 environment other than the environment used by Operations.
The DCS shall provide the capability to execute diagnostic tests for verifying proper
- DCS-358 operation of system capabilities and components.
- DCS-359 The DCS shall provide the capability to support end-to-end testing of DCS functions.
The DCS shall provide the capability to support software maintenance during normal
- DCS-360 operations on a non-interruptive basis.
The DCS shall provide the capability to support preventive maintenance during normal
- DCS-361 operations on a non-interruptive basis.
The DCS shall provide the capability to support operator training during normal operations
- DCS-362 on a non-interruptive basis.

- DCS-219 Transferability / Conversion
- DCS-220 Other Requirements
- DCS-221 Operations
- DCS-222 Site Adaptation