Unix Hosting Service-Level Description

STANDARD SERVICE DESCRIPTION	
Physical Facility Services Location: □ Building 12, Room 1100 □ Qwest Facility in Sterling, VA	• Data center temperature and humidity maintained within conventional, vendor recommended limits for computing and telecommunications equipment. • Sufficient power for all installed equipment, with an uninterruptible power supply and standby generator to maintain normal business operations during a utility outage. • Physical security of the computer room with bio-metric and badge controlled access limited to approved personnel. • Security guards at entrance for Operations staff 24x7. • Facility monitored by video cameras. • Monitoring systems for detecting water leaks, smoke and fire as well as a fire suppression system
System Administration Services	• Ongoing administration including management of user accounts and management of storage on the equipment provided. • Timely diagnosis and resolution of hardware and system software problems within the limits of vendor provided assistance.
Monitoring Services	• Hosted Services are monitored 24 hours per day, 7 days per week. • Monitoring includes hardware status and system performance (e.g., CPU, memory, disk space utilization, services, selected ports and processes). • System problem diagnosis/resolution by systems experts either on site or on call. • In the event an adverse incident is detected by system monitors, CIT will contact the Customer as per the Customer requirements.
Operating System and Utility Software Services	• Operating system and supported utility software installed and configured following CIT standards. Tuning and custom modifications discussed and implemented upon completion of technical review and impact analysis. • Operating system upgrades and patches to versions fully supported by the vendor and compatible with application software. Upgrades to be done on a schedule acceptable to both CIT and the Customer. • Regular updates and upgrades of other CIT-provided software at times which are coordinated with the Customer. • Security patches applied to CIT-provided software in a timely manner coordinated with the Customer.
Security Services	• Basic protection of hardware and software through NIH border firewalls and network intrusion detection in accordance with the data center security architecture. • Secure management in accordance with the Federal Information Security Management Act (FISMA), NIST guidelines, Certification and Accreditation (C&A) security review and SAS 70 audit review. • Host-based security solutions installed, maintained, and monitored to prevent system compromises (e.g., virus infections, intrusions, etc.).
Backup Services	• All backups administered in accordance with CIT standards and Customer requirements. Backups of Customer-managed applications may require additional coordination with the Customer.

	• In the event of a system problem causing loss of data, CIT will restore data from the most recent backup. In the event of an accidental deletion or corruption of data by the Customer, CIT will restore data from the Customer requested backup date. • Daily incremental backups of system data; monthly backups of system data to tape and taken offsite. • Onsite backup library data copied across private network to offsite library located in secure data center (Sterling). • Application data backed up as coordinated with application owner. Database backups are performed only as coordinated with database administrators (CIT or customer as appropriate). Other data is backed up by default. • Default backup retention is such that the current copy will remain in the backup system as long as it does not change. Prior versions of files are kept by default for 6 weeks. The length of time prior versions are maintained and the number of prior versions that are kept can be coordinated.
Hardware Services	• Preliminary consultation with the Customer to determine needs and performance requirements, leading to an agreement on equipment to be provided for the Customer's use. • Additional meetings with the Customer, as needed, to revise equipment requirements based on changing business needs and/or new technical requirements. • Equipment acquired and configured to meet identified Customer requirements. • Timely delivery of equipment when needed. • Consult and coordinate with the Customer on equipment refreshes.
Server Hosting Server Specifications □ **If contracted**	____: 2 Processor Commodity Sun Server(s) ____: 4 Processor Commodity Sun Server(s) ____: Entry-level Multi-core Commodity Sun Server(s)____: Custom Server(s) Specify:
Software Specifications	Operating System: □ Solaris □ HP Unix □ Tru64
Managed Storage Services □ **If contracted**	• Storage is provided in a redundant configuration as coordinated with the customer. • Space provided on a SAN is billed based on the amount allocated to the customer.
Application Firewall Services □ **If contracted**	• Application firewall services are provided to meet specific Customer security requirements. Customer collaboration is required to establish application security architecture and to create and review firewall rule sets.
Local Traffic Management Services □ **If contracted**	• Provides load balancing and SSL acceleration support through the use of BigIP F5 devices. • Provides unique load sharing and failover support for customer applications and servers through application server pooling and custom rules. • Provide SSL digital certificates to customers through arrangements with Verisign and the HHS PKI program to authenticate application servers.

Disaster Recovery Services □ **If contracted**	• In collaboration with the Customer, prepare, implement, and test a disaster recovery plan within the scope of the NIH Computer Center disaster recovery program as described in the Computer Center Disaster Recovery Plan. • Provision of off-site data storage and warm site availability. • Provide Oracle Database and Middle Tier disaster recovery services per agreement. • Recovery of the Customer's systems in case of a disaster in accordance with the disaster recovery plan.
Apache Web Hosting Services □ **If contracted**	[Descriptions to be added upon rollout of this future service]
SERVICE AVAILABILITY	
Service Coverage	• CIT will provide coverage for the Hosted Services, 24 hours a day, 7 days a week. See the contact personnel listed in Appendix A for the CIT emergency after business hours contact(s).
Service Availability	• CIT will provide 99.9% system availability within the agreed service hours. • CIT will provide 99.9% availability of resources to support services, exclusive of scheduled maintenance activities. • Installation and configuration of services within time frames agreed to with the customer. • If CIT is unable to meet system availability target levels due to CIT/DCSS negligence, CIT will provide the Customer reimbursement for unavailable services based on a calculated formula, upon request.
SERVICE OPERATIONS	
System Monitoring and Support	CIT will manage and monitor the servers, which are part of the Hosted Services, 24 hours, 7 days a week.
System Maintenance	All services and/or related system components require regularly scheduled maintenance ("Maintenance Window") in order to meet the establish service availability levels. These maintenance window activities will or may render the systems and/or applications unavailable for normal user interaction for the following locations and timeframes: **Type:** Scheduled Maintenance **Location(s):** Data Center Building 12 **Timeframe:** Dependent on type of maintenance **Notification:** • Coordinate with the customer as needed prior to the scheduled maintenance window • Will specify the servers and location affected If services and/or related components require emergency maintenance in order to meet the established service levels, CIT will conduct the following activities: **Type:** Emergency Maintenance **Location(s):** Data Center Building 12 **Timeframe:** Dependent on type of emergency **Notification:** • Will immediately attempt to notify the Customer as requested

<table>
<tr><td></td><td>• Will specify the servers and location affected
• Will coordinate with the Customer to develop a priority scheme if a shut down of servers is necessary</td></tr>
<tr><th colspan="2">SERVICE DELIVERY</th></tr>
<tr><td><b>Service Delivery Metrics</b></td><td>• Delivery of Unix server(s) to customer: Dependent on the customer’s implementation timeframe and time to procure custom server requests
• Backup Restores: Based on customer’s urgency and dependent on customer’s retention needs</td></tr>
<tr><th colspan="2">CUSTOMER SUPPORT</th></tr>
<tr><td><b>Response Times</b></td><td>• For non-emergency calls, CIT will provide the appropriate call-back response as indicated on the ASR service request ticket.
• Emergencies will be handled within a 1 hour call-back window after receiving a service request ticket.</td></tr>
<tr><td><b>CIT DCSS Management Escalation Contacts</b></td><td>
<table>
<tr><th>Name</th><th>Title</th><th>Contact Number</th></tr>
<tr><td>Paula Moore</td><td>Unix Team Lead, Hosting Services Branch</td><td>301-402-1237</td></tr>
<tr><td>Laura Bennett</td><td>Branch Chief, Hosting Services Branch</td><td>301-435-5493</td></tr>
<tr><td>Adriane Burton</td><td>Director, Division of Computer System Services</td><td>301-451-4553</td></tr>
</table>
</td></tr>
</table>