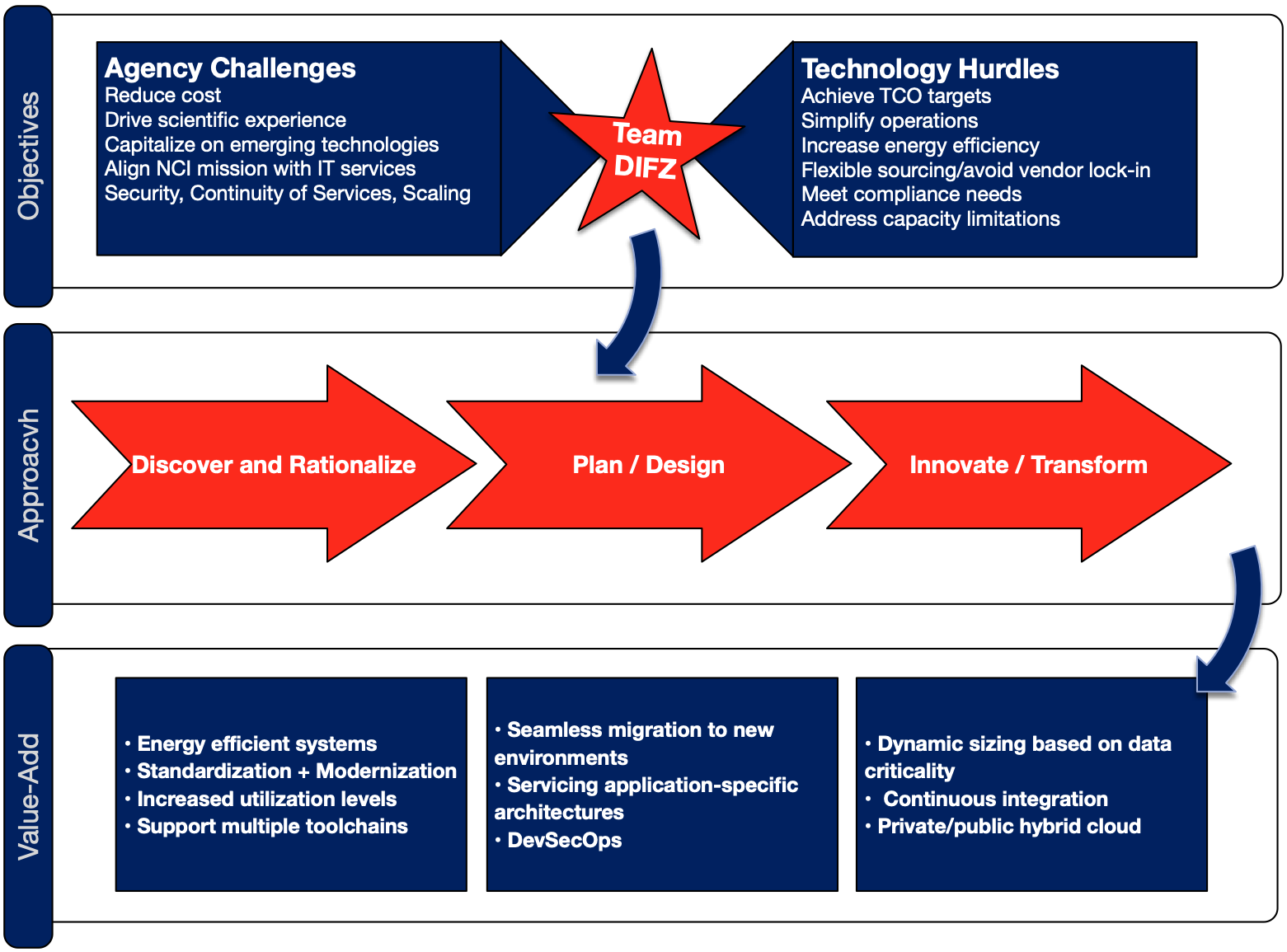
# Option A - Hardware Sustainment and Backed-Up Data Storage

Team DIFZ will to maintain the CTEP infrastructure at the NIH or NCI data center following all agency data center requirements, SOPs, technical guidance, and regulations. To do so, we will take a proactive, collaborative approach. See the following exhibit, that captures our vision of a best practices model that begins with a focus on operational efficiency and professionally driven system and network administration. Working together, the Digital Infuzion team is able to design, manage, and operate data center infrastructures, including facilities, computing assets and storage networks and server infrastructure, to optimize the performance and efficiency of the entire data center.

To ensure best-in-class equipment,Team DIFZ will provide and maintain all equipment that is necessary for CTEP-ESYS environment or service that is not provided by data center. It is expected that hardware refresh by our team will take place at a minimum every 5 years from date of purchase or as required for hardware that has reached End of Service/Support Life (EOSL) or where newer software/operating systems that will not operate on an older server. All hardware purchases must meet NIST standards (e.g., may not purchase or supply servers from companies listed on the Federal No Buy List).

Some of the tasks we will be responsible for include: managing all CTEP-ESYS related equipment including shut down and restarts; maintaining documentation of the inventory in a manner approved by the COR, using our configuration management database; maintaining responsibility for capacity planning to ensure that the equipment is adequate to maintain the high availability of the systems deemed vital to CTEP operations.

Exhibit. Team DIFZ proposes an actively managed solution for maintaining all systems is necessary for the CTEP-ESYS environment

Security is paramount, and in the data center security, Team DIFZ utilizes a comprehensive set of policies, precautions and practices adopted to avoid unauthorized access and manipulation of the data center's resources. We understand that providing a proper security system is critical because this data center houses NCI critical data, applications, and systems. We mitigate the risk of security issues in the data center with our NIST-based framework that informs the SOPs used to ensure proper security protocols are enabled for all of the equipment and systems in the data center. We thus help the agency avoid reputation damage and loss of trust from researchers and others who rely on these assets by bringing our substantial cyber security expertise to bear, preventing breaches. We do this by implementing data center physical security measures beyond the outer layer of defense the physical site provides, such as server cage locks, disabling USB and other port connections to systems and the network, and address Internet-of-Things vulnerabilities. We audit to ensure default router settings have been changed (and documented in the CM database), disconnect IoT devices when they are not needed, and keep software, firmware updated,

When designing a data center, we are intention in planning out the physical space. This includes deciding whether the data center to be in a secluded location or a more populated area, being conscientious of weather-related dangers and low-lying areas (floodwaters and technology aren’t a great mix). If the center is sited in a more populated area, we can recommend “hiding in plain sight” by having the facility blend in with its surroundings. We will audit a current service provider’s facility to check out the construction and location of their building, and request compliance reports to see how they measure up. Our team will be trained on and adhere to rules of behavior specified in the NCI Data Center Policy and Work Rules document.

For example, while Universal Plug and Play (UPnP) has its uses, it can make printers, routers, cameras and IoT devices vulnerable to cyber attacks. The principle behind designing UPnP is to make it easier to network devices without additional configuration and help them automatically discover each other. However, this benefits hackers more than anything as they can discover all IoT devices beyond your local network. Therefore, we recommend turning off UPnP completely. We also double check to ensure security agents are operating and current on all servers.

Facility safety means we will shut down any CTEP-ESYS provided equipment if our team detects that it   
presents a hazard, is doing harm to, or has harmed the facility.

Monitoring — Team DIFZ will monitor all CTEP-ESYS provided equipment using a combination of software agents deployed on servers to keep track of application uptime, database health, and system integrity. We will also monitor the network, routers, firewalls, and other communications and internet working gear to provide a real time map of the status of the network. We will build out a monitoring dashboard that provides summary status information on these systems, with drill-down into detailed status screens. We will provide automated notifications from the dashboard to all appropriate stakeholders. To ensure effective implementation and control of operational activities, we employ a CMMI Level 3 set of processes. This ensures efficient, safe, and reliable (and repeatable) processes. We use Nagios and other automated monitoring tools to ensure we are cognizant of status of all equipment, systems and subsystems. This is of particular importance for network monitoring and security. As part of the team's continuous improvement philosophy, we realize that operator knowledge and performance are critical to support safe and reliable systems and network operation. Our staff improvement plan and choice of team members with proven track record ensures that lessons learned from other engagements, as well as industry best practices, will be brought to bear in relation to operation of the customer's environment.

Team DIFZ will work with the COR as directed to seek opportunities to improve the operational effectiveness of the data center environment (e.g., other hosting models) and recommend alternatives to safeguard the CTEP IT infrastructure, increase system performance, and/or increase cost savings. Our reporting will be key performance indicator (KPI) driven. For example, for data center O&M, the most important metrics include:

* Capacity factor – Relates actual systems or equipment operation to the full-capacity operation. This is a measure of actual operation compared to full-utilization operation.
* Change requests or trouble tickets generated/closed out – Tracking of tickets generated and completed (closed out) over time allows the manager to better understand workloads and better schedule staff.
* Backlog of corrective maintenance – An indicator of workload issues and effectiveness of preventive/predictive maintenance programs.
* Energy use and other environmental indicators – A key indicator of equipment performance, level of efficiency achieved, and possible degradation. We have learned from NOC/data center O&M engagements that failure of equipment can be reliable predicted by monitoring of environmental factors.
* Inventory control – An accurate accounting of spare parts can be an important element in controlling costs. A regular reconciliation of inventory “on the books” and “on the shelves” can provide a good measure of cost control practices.
* Level of Effort, projected vs actual – Weekly and monthly activity reporting, workload, scheduling, and economic implications (such as EVM).
* Absentee rate and staff turnover– A high or varying absentee rate can be a signal of low worker morale and should be tracked. In addition, a high absentee rate can have a significant economic impact. High turnover rates are also a sign of low worker morale. Significant costs are incurred in the hiring and training of new staff.
* Other costs include those associated with errors made by newly hired personnel that normally would not have been made by experienced staff.

From a back-office perspective, we look at life cycle costs and simple payback (the ratio of total installed cost to first-year savings) as means of measuring the impact of O&M investment, so stakeholders can make informed decisions. In addition to SOW Task 2: System Back Up, Team DIFZ will leverage the ITSM approach, and ensure backed-up data stored at these locations is available in such a fashion as to ensure rapid recovery of CTEP-ESYS services to meet the SLA requirements. We will design a storage area network (SAN) solution to provide backed-up data storage with capacity to hold up to one year of data in a secure location no less than 25 miles physically away from the primary data center (e.g., tapes or high-capacity removable hard disk drives at a secure remote facility).

# 2. Option B - Primary Data Center Migration Services

Team DIFZ will provide Data Center Migration Services required to move servers and operating systems (both physical and virtual environments), storage hardware, tape libraries, and ip console switches from their current NIH data center location to a new data center location (e.g., NCI). Our approach to moving to a new Data Center deployment includes deploying several components that help the data center to be secure and accessible, inventorying the systems to be moved: storage systems, routers, firewalls, switches, and servers. It also includes the deployment of application delivery controllers such as computer network devices.

The Team DIFZ strategy is based on understanding the precise definition of the objective of why we are migrating the data center. We then work upfront to develop careful budget planning. The team applies our knowledge of the process, leveraging individuals who have experience and training in the migration process. For a successful migration, the first step is to know about the data center. This is Phase I – Application, Data Architecture Discovery and Mapping. We need to assess the data center based on its network, server, and operating system requirements. We evaluate the applications supported by the data center.

The next step is to build a strategy for a successful migration process. This is Phase II – Migration Plan, and it includes documenting: the equipment needed, connectivity diagrams, cooling infrastructure, space utilization, and power specifications, etc. We then select destination for the migration — starting with power and cooling infrastructure, then cabling and network controller locations, then racks and servers, power up, and, finally, cloning of systems onto the new deployments. This depends on various factors: the storage space required, the power required, security, and the physical location of hardware assets. We then conduct a design review of the process, and to consider all the stakeholders and technology in the review. We will ensure in our project management plan (PMP) that all the requested steps in the SOW will be incorporated into the Team DIFZ migration effort.

Validation of our migration plan includes: ensuring physical infrastructure is to support the processes.; a review the elements of infrastructure to avoid last moment changes; conducting benchmark and reviews of application performance; and, system owner sign-off. Post-migration verification ensures services which were running before the migration process execution are now running the new environment. We also need to verify all software and data is scrubbed from the previous facility.

# 3. Option C - Secondary Data Center Migration Services

Team DIFZ will be responsible for the identifying, prioritizing, provisioning in the new environment, performing a safe and secure migration, testing and certifying of all applications and related equipment from the current data center to the new environment. In addition, we will assess if the existing data centers have additional requirements that need to be met per current hosting model requirements. Team DIFZ will be responsible for each phase of this migration (meeting the same requirements as Option B). We will undertake the steps required to migrate servers and operating systems (both physical and virtual environments), storage hardware, tape libraries, and IP console switches from their current NIH (Sterling, VA) data center location to a new data center location (e.g., NCI).