The DIFZ Team brings experience working with a wide variety of Federal Agencies to implement their information security programs. The examples below from DIFZ and teaming partner PPD demonstrate our experience and extensive IT security expertise and resources that we have deployed in Federal contracts. We will promote improved and expanded IT governance for effective IT management, enterprise-wide organizational change management processes for strengthened security and improved services, strong project management through our program management office (PMO) support for CIOs uses earned value measurement and tracking, and a sound centralized approach for migrating to a single CIO IT infrastructure. Team DIFZ consolidation benefits include reducing IT operation costs; freeing resources for CIO support; reducing procurement and IT costs by leveraging enterprise buys on standard platforms and applications; strengthening cyber security through standardization, and reducing trouble resolution time through the use of automated, advanced keyboard-to-keyboard processes.

**Integrated Security Architecture.** DIFZ has provided IT security-related research and engineering support to the Centers for Medicare and Medicaid Services (CMS) Information Security and Privacy Groups’ (ISPG) DevSecOps (DSO) Team in compliance with HSPD and FISMA since 2016. As part of ISPG’s DSO Support Team, DIFZ plays a key role in the development of high-value DevSecOps-related solutions that ensure security is “built-in” throughout all phases of each CMS system’s life cycle. Supporting the CMS CISO’s development of DevSecOps approach DIFZ successfully design and demonstrates ISPG’s DevSecOps automation solutions which have assisted with the modernization of the CMS ATO process through automated security compliance testing and documentation through integration of security testing tools into existing CI/CD pipelines. Through automation, the DIFZ DSO solutions team help promote continuous code validation, change, and configuration management.

Development Teams and ISPG Assessors analyze security data to generate accurate documentation at each Sprint/Release and support faster ATO decisions. The DIFZ Team integrates security baseline hardening and compliance testing into the CI/CD pipeline for cloud applications through development and integration of Chef InSpec Profiles, an open-source framework for testing and auditing applications and infrastructure, into those existing DevSecOps pipelines. Developers maintain agile code delivery, while satisfying compliance requirements and improving internal Security Impact Assessments (SIA). The DIFZ Team also supports development of data protection solutions at rest and in transition that include cost-effective strategies for encryption, secrets management and access control, leveraging existing investments at CMS.

**Security Technology Infrastructure.** Our teaming partner PPD has experience providing secure data center services; their two primary data centers (in Durham, NC and Austin, TX) house the infrastructure that hosts applications used to support the clinical trial process and corporate support functions. These data centers are built to specifications to ensure physical security, hardened to prevent intrusion, and supported by back-up power sources. Their production data center is compliant with HIPAA, Federal Information Security Management Act (FISMA) (High), FedRAMP, ISO 27001, and Payment Card Industry Data Security Standard (PCI DSS) standards. Standardized processes ensure data is backed up. All back-ups are replicated between the two data centers. Only authorized IT staff or facilities staff have data center access. Visitors must be escorted by authorized staff.

**IT Security Plan.** DIFZ Team recognizes that secure physical facilities integrated with strong IT infrastructure, data, and document storage are keys to sensitive data protection, project communications, cost control, and an enhanced user experience. Our strategic investment in technology creates the backbone for communications, management, processing, and storage of data. Robust facilities and a computing infrastructure built on best practices and industry-standard hardware and software result in secure and efficient administration of communications, data collection, data management, and storage requirements for hundreds of studies.

Information security risk assessments are completed on external vendors to ensure they have the appropriate controls in place. Information security risk assessments are completed on systems that include relevant responsibilities for review, scope, frequency, risk mitigations actions and approval. SOP IT-04 (Computer Room and Data Security) includes the high-level requirements and process for data backup and recovery. Additionally, WPDs detail the process by specific OS. Test restores are required at least semi-annually for each type of back-up application. Back-up and disaster recovery procedures follow the Disaster Recovery Master Plan, SOP IT-05. Databases can be recovered based on the use of offline backup/recovery, online backup/recovery or logical back up/recovery techniques. Additionally, systems requiring 24x7x365 availability implement high-availability strategies.

**Security Environment.** DIFZ Team operates under standard policies and procedures that provide a framework for information security. We use best security practices as a basis for our information security program and a defense-in-depth strategy to assure confidentiality, integrity, and availability of our sponsors’ sensitive data. Their environment is composed of computers, operating systems, applications and services, networks, operations and monitoring equipment, and specialized hardware, along with the administrative and operations staff required to run and maintain the services. The data centers are also included as part of their security posture; all data center services and physical access have safeguards in place to deter from any malicious or accidental damage.

The DIFZ Team chose to adopt the ISO 27001 framework due to the global nature of our provided services, receiving ISO/IEC 27001:2013 certification in 2020 and recertification in 2021.

**IT Security Policies and Procedures.** The DIFZ Team operates under a standard set of policies, SOPs, Best Practices & Guidelines (BPGs) that provide a framework for our information security environment. The DIFZ Team can provide a full listing of these policies, SOPs, and BPGs during competitive range negotiation responses.

Team DIFZ is fully prepared to provide support for the protection of critical infrastructure, information assurance, and implement cyber security protection. Our approach ensures confidentiality, integrity, availability, accountability, restoration, authentication, non-repudiation, event response, and other capabilities. Based on our experience with multiple clients, the team understand that the government's networks and critical infrastructure must provide a secure and readily adaptable and manageable foundation to enable the applications users expect, while ensuring high performance and reliability. Our team's goal with infrastructure operations is to ensure network functionality that:

* + Reduces complexity while improving security;
  + Increases security while addressing cost-effectiveness;
  + Enables collaboration and unified capabilities, particularly with access to mission-specific applications;
  + Extend the operating environment to meet consolidation demands and enhance user productivity;

And, address new possibilities such as cloud services and applications with sophisticated architectures that optimize and accelerate LANs and WANs and integrate networking, storage, and management solutions "BYOD" and mobile computing, and other new-horizon IT challenges.

Team DIFZ will accomplish this with trained, highly competent support staff and proven consistency of processes and procedures for the operations, maintenance and support of the critical infrastructure systems. The the OCIO infrastructure is generalized in the following exhibit.

Network, systems, and software problem analysis, testing and patch creation/installation are at the heart of our O&M approach and experience. Patch management and server administration are critical components that require robust dependable and repeatable processes. Included in our processes will be vendor product license management. For mission-essential applications, in particular, it is important that all servers are patched and maintained in order to keep the system operational for the users and to maintain security. In addition, certification of applications and other solution components will be critical. Team DIFZ has extensive experience providing these critical services for our customers. LAN and WAN optimization are paramount to infrastructure hardening — our team brings the needed broad perspective and understanding of the dynamic relationships between physical and virtual servers, systems, network, and storage resources, as well as the customer's unique environment and mission needs.

Most importantly, our team has engineered networks that are readily adaptable to continuously incorporate innovative new functionality and keep pace with ongoing transformations in how users access their services and how applications are consumed. Our ability to bring new ideas to the customer include considering technologies such as Converged Network Fabric (collapsing LANs and SANs into a single common network infrastructure), or OpenFlow (virtualizing the network) enable greater flexibility and cost-effective deployment of redundancy into the network architecture.

Team DIFZ, at \_\_\_\_\_\_\_\_\_\_\_\_\_, engineered a network is not only adaptive, but also intelligent — providing 360 degree visibility and pervasive control, as the network itself enforced security policies. We successfully deployed the very monitoring solutions we recommend for the customer, and our engineers apply both indicative and preventive technology automation throughout network environments to enable consistent monitoring and automated alerting. Recognizing adverse trends and security events leads to increase security and availability while reducing service interruptions and avoiding critical incidents.

We see the opportunity here to lower costs and increase energy efficiency. Our team is committed to green technologies and aims to build networks that can monitor and manage energy usage and carbon emissions. With our infrastructure operations, the government is able to meet the evolving requirements of consolidation quickly and cost-effectively. The government will immediately see gains because we can quickly deploy applications, easily scale and adapt services, and simplify and improve the task of network management with our "hit the ground running" approach, leveraging the value of network engineering by our experienced team.

In conjunction with the EA and through our COE, we will support the development of Disaster Recovery Plans and Contingency Plans to protect the OCIO IT investments in accordance with DOE direction, as well develop and maintain data center configuration drawings.

Team DIFZ fully understands the scope of services sought in support of the OCIO. The adjacent text box highlights a sample of Team DIFZ's compelling history of relevant experience and capabilities. In all such engagements, our service delivery incorporates, and is conducted in accordance with, the latest revisions of NIST Special Publications (SP) 800-18, 800-37, 800-39, 800-53, 800-53A and other relevant NIST documents/publications. In fact, members of Team DIFZ have made use of Security Policy with NIST in the areas of computing, configuration management, software assurance, accreditation and authorization of systems, cloud computing, mobile bandwidth constraints, FIPS 140-2 and draft FIPS 140-3 leveling. In this way, we offer our clients advance insights into emerging trends and standards and will do the same for FRA as our approach and technologies already incorporate expected updates from NIST SP 800-53, revision 4.

Team DIFZ will provide IT Security implementation support services to complement the OCIO responsibilities for planning and managing IT cyber security policy and its implementation, awareness and training, security oversight and compliance, critical infrastructure protection and other requirements that may arise through the duration of this contract. Team DIFZ will provide Certified Information Systems Security Professionals (CISSPs) and maintain those certifications during the performance of the services in this area.

Team DIFZ will bring our experience from \_\_\_\_\_\_\_\_\_\_\_\_ in developing and implementing cyber security programs which educate users on computer security issues, provide for disaster recovery, and provide for continuity of operations. Team DIFZ will provide for contingency planning, and, as described elsewhere provide means to detect intrusion (e.g. hackers, advance persistent threats, malware/virus detection). Building on our experience at \_\_\_\_\_\_\_\_\_\_, we will provide support for containment, recovery and reporting including lessons learned. Team DIFZ will provide risk assessments. Our goal is a cyber security risk management that will balance operations efficiency and effectiveness with acceptable risk. Finally, we will support the IT Certification and Accreditation process.

One advantage of Team DIFZ’s approach: continuous monitoring ensures fast response. Many organizations tend to associate monitoring with periodic security assessments, reauthorizations, data analysis and associated reporting. Such passive activities are valuable, but simply not sufficient in today’s world of sophisticated hackers and Advanced Persistent Threats (APTs). NIST SP 800-53 defines the technical security controls needed to implement an effective continuous monitoring program. In particular, this standard advocates “malicious user testing, penetration testing, red-team exercises, and other forms of security testing.” Such proactive testing of physical and technical controls is necessary and represents critical components of an effective continuous monitoring program. Any provider that does not include such services as part of their offering would not be compliant with NIST standards and the associated requirements of the government’s SOW/PWS. More importantly, they would leave the agency vulnerable to APTs and other malicious attacks.

Team DIFZ has adopted and applies the recommended standards of NIST SP 800-137 to assist organizations in developing a continuous monitoring strategy and implementing a related program. According to this standard, NIST describes continuous monitoring as helping to “ensure ongoing situational awareness and control of the security of systems across the organization and ongoing knowledge of associated threats and vulnerabilities, despite inevitable changes to organizational information systems and their environments of operation.” (NIST SP 800-137, page 6). Team DIFZ intends to use Tenable's SecurityCenter Continuous View as an integrated vulnerability management solution — it gives organizations the ability to continuously correlate, evaluate, and anticipate their business risks in accordance with NIST SP 800-137. Tenable's COTS product will enable the OCIO to continuously test the network’s resistance to attack: identifying, proving and tracing exposures to critical assets. Tenable's COTS product will enable our team to automate testing against critical IT assets, find vulnerabilities in FRA systems and enumerate connections and potential attack paths. Security test results are centralized in the solution’s Dashboard and aggregated in Campaign, Trend and Executive Summary reports; allowing managers and executives to easily assess their organization’s security posture. Key Insight capabilities include:

* + Predictive attack path planning leverages patented AI algorithms to show how an attacker can take advantage of weaknesses to get to your most critical assets
  + Multi-vector risk analysis to predict how a real attack could occur through a weakness in your web applications and lead to a breach of critical data in your network
  + Automated security testing to continuously and proactively assesses the security of your organization’s most critical IT and business assets.

Open API that provides the ability to integrate with other technologies used within the ecosystem to add intelligence to the data produced by vulnerability scanners, Security Information and Event Management (SIEM), Data Loss Prevention (DLP), and Governance, Risk, and Compliance (GRC).