The DIFZ Team brings experience working with a wide variety of Federal Agencies to implement IT infrastructure and information security programs. Network infrastructure Security, as applied to government IT environments, is Digital Infuzion’s process of protecting the underlying networking infrastructure by installing preventative measures to deny unauthorized access, modification, deletion, and theft of resources and data. In addition to the core services for interface with the network operations center (NOC), we will implement the customer’s security program in compliance with government directives, HSPD, and FISMA. Primarily, the DIFZ Team will undertake implementation and upkeep of government data center components, protection of the data and respective applications from internal and external threats, and establish continuity of operations mechanisms for efficient restoration of government operations after a security incident. Our security approach relies on risk assessment in keeping with NIST’s recommended approach, proactive monitoring, and the formation of quick-response teams with forensic expertise so that we can mitigate the fallout from any potential security breach.

The examples following, from Digital Infuzion and our teaming partners, demonstrate our experience and extensive IT security expertise and resources that we have deployed in Federal contracts. Team DIFZ has experience with government legacy network/data center consolidation efforts as well as transition to cloud services; cloud computing; experience with other government enterprise solutions/databases such as \_\_\_\_\_ applications and \_\_\_ database management systems. Additionally, expertise with Microsoft Office (i.e., Excel, Word, PowerPoint); verbal and written communication skills to clearly communicate with the government NOC POCs; and having a self-directed ability to work solo and collaboratively in a team environment or with the government management, peers, and customers are essential. Team DIFZ understands NIST 800-series frameworks for security self-assessments, having conducted A&A/C&As and other audits at several federal agencies. We will recommend processes that have been tried-and-tested so that formal written documentation is available to notify the data center of any changes in needs or requirements. Through the help desk, we will provide current contact and escalation information for the Federal Sponsor of any applications and the Technical Project’s lead. This is an automated process, when a ticket is opened. As communication is a cornerstone of the Team DIFZ approach to SOW 5.2.1.1 Requirements and Service, we will convene daily standup meetings so that our team consolidates all change requests and documents outstanding issues; we will then notify the data center of any changes in needs or requirements. We will submit service requests as per data center policy, and not call the on-call phone number for general support, reserving its use for critical emergencies.

To ensure SOW 5.2.1.2 Software is provided and maintained as necessary for the government environment and services not provided by the data center, Team DIFZ will integrate support with a well-documented configuration management process, patch management, and version control. Understanding what applications are in the environment is the cornerstone, and Team DIFZ will update the government’s inventory of applications, ensuring accurate information about licenses, deployment environments, versions, known vulnerabilities, and the user base for each. Software is central to the government, for researcher support. Managing the software asset requires processes that are easily adaptable and robust.

Team DIFZ will maintain and update government developed software, COTS software configurations, and software systems. We will implement software configuration management (CM) procedures to provide a uniform approach to supporting government and other custom developed systems. We will assign a software configuration manager to educate organization stakeholders on CM “best practices,” develop and maintain CM procedures and work instructions for each product assigned. We will only employ software that has vendor or community support, per agency policy. The DIFZ team will establish release baselines and work with the development and data center teams in administering CM repositories. The Team DIFZ process for maintaining and updating software includes the development and maintenance of artifacts following proper version control procedures using CMMI-L3 compliant CM processes and work instructions. We will work with the the government governance body for reviewing and approving change requests under CM procedures and work instructions.

Team DIFZ will comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes (see https://www.hhs.gov/sites/default/files/eplc-policy-dec- 2016.pdf), and agency Enterprise Architecture requirements to ensure information is appropriately protected. We acknowledge that all information systems development or enhancement tasks will follow the agency EPLC framework.

Our overall development methodology is hybrid of a waterfall approach modified with Agile practices — as applicable to the complexity of the requested development effort or enhancement, as well as adapting a more iterative agile approach for change requests needed on an expedited basis. building and maintain in stable and secure applications. As we discuss under CM, we will document government equipment configuration and specifications. Our systems engineers will manage all government equipment including shut down and restarts and provide remediation (tier 3) for all government application and service issues.

Exhibit x. Making Changes to Software. The development process needed to support minor enhancements and defect resolution mirrors a larger system life cycle, but is scaled back depending on the scope of specific enhancements.

| **Type of Change** | **Methodology** |
| --- | --- |
| **Minor Enhancement** | |
| Enhancements that require less than 40 hours of labor and are therefore scheduled as part of normal support operations. | Follow all phases and documentation requirements of the normal SDLC. |
| **Bug Fix** | |
| Small software patches to correct defective code. | Include only the Version Description Document (VDD). |
| **Proof of Concept** | |
| Development of prototypes to validate new technologies, architectures, and business requirements prior to commitment of significant resources. | Conduct abbreviated requirements and development phases of the SDLC. Requirements must be documented, but do not require a formal Systems Requirement Document. Example: create site-flows / web pages to describe how the application would work in an informal way. |

To perform all application deployments, Team DIFZ will follow the government procedures for rolling out a tested and approved application. Deploying software to production correctly is a challenge. Bad deployments can lead to delays and even downtime. Being in charge of a deployment process is a big responsibility as well as a huge challenge. Modern software deployment involves many moving parts across the organization and its toolset. For this, we will document the release to production with a plan. Creating a deployment plan is an opportunity to get insight from all stakeholders. Once the plan is in place, it provides crucial information and instructions for the entire deployment. Plans may involve both manual and automated testing at each deployment stage. Risk analyses, checklists, responsibilities, and contact information for each stakeholder also play a role. The plan should be reviewed and approved by all stakeholders.

As discussed under CM, we have demonstrated that Team DIFZ recognizes how coherent versioning and release notes contribute to good documentation, especially as we plan on the use of a versioned documentation system Furthermore, being able to associate any issues with the correct system is valuable for support. We do this by creating a formal release or tag in the version control system (Git or otherwise). This means we can enable bug trackers to associate issues with specific versions.

We will also formulate a Rollback Plan because sometimes even the best organized deployments can fail. If the production environment goes down after a deployment, often the best course of action is rolling back to the previous version of the software. Being able to do so quickly makes all the difference to getting the production environment back up and running — integral to Team DIFZ’s DR approach.

To ensure Facility Safety, Team DIFZ will update existing engineering support SOPs so our staff have clear guidance on managing systems in a safe manner. For example, upon detecting any unauthorized equipment (that is, not provided by authorized vendors or the government), we will shut it down if it presents a hazard, is doing harm to, or has harmed the facility. When working on hardware within the Data Center, we will adhere to the government or the government Data Center Infrastructure Guidelines for infrastructure rack, wiring, tools and labeling, and naming standards. Our staff, as part of the onboarding process, will be training in all government or the government Data Center Policy and Work Rules so no behavior strays outside of those requirements.

## System Security

DIFZ has provided IT system security-related 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.

For any hybrid Agile development, release teams and information assurance experts 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.

Our teaming partner \_\_\_\_ has experience providing secure data center services — their facilities 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.  We will maintain the SAML Single Sign-on (SSO) federated standard to exchange user identity and authentication information between the CORE systems and other information sources for government Clinical Trials (e.g., NCTN group websites). Team DIFZ will work to expand SSO services for new websites/web-based systems as approved.

There are three essential roles in the government Certification and Accreditation Process (CAP). At a minimum, a system owner, Designated Approving Authority (DAA), and certifying agent are required to implement the process. Team DIFZ has experience at The government with the phases of the C&A process: Initiation, Security Certification, Security Accreditation, and Continuous Monitoring. Each phase consists of a set of defined tasks and subtasks that are to be performed by responsible individuals (e.g.,, system owner, Certifying Agent, user representatives, etc.). Security certification and accreditation activities can be applied to an information system at appropriate phases in the system development life cycle. Additionally, the activities can be tailored to apply a level of effort and rigor that is most suitable for the system undergoing security certification and accreditation. The fundamental purpose of the certification process is to determine if the security controls for the IT system are correctly implemented and are effective in their application. Certification levels establish the level of effort and test methods to be used to verify security controls for security test and evaluation efforts.

The 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. 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 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.

## 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. We will install software vendor released security patches, update the antivirus definitions to permit automatic updates, and remediate critical and high vulnerabilities in an expedited manner, within agency specified timeframes. Notification of routine updates will occur as part of standard Change Management. We will report any potential security breach in accordance with agency-specific incident response procedures. For example, we will notify the CO, PM, and COR within one-hour, upon realization of any potential security breach.