McLeod Information Systems LLC

Supporting our client's goals to balance security and operability

ABOUT US

WWW.MCLEODIS.COM

McLeod Information Systems, LLC is a comprehensive cybersecurity services company. Our staff has over 25 years of experience servicing and supporting federal organizations including Defense Information System Agency (DISA), Department of Defense (DoD), Housing and Urban Development (HUD) Office of Inspector General (OIG), Veterans Affairs (VA) and commercial industries to include Real Estate (agents and brokers), CPA firms and Law offices. Our team has decades of experience servicing complex, multifaceted IT Security needs in warfare, private industry and government. MIS is a Service Disabled Veteran Owned Small Business (SDVOSB) founded in 2016 and is headquartered in North Charleston, SC

MISSION

Provide our clients the peace of mind that their information is processed and protected in a secure infrastructure. We accomplish this by accessing process and procedures to implement security controls that mitigate risk.

VISION

Support our client's goals to balance security and operability to provide a service to their customer that is profitable and rewarding.

CORE COMPETENCIES

- Assessment and Authorization Support
- Security Control Assessment
- Process Development and Improvement
- Consulting
- CUI Program Support
- Staff Augmentation

PAST PERFORMANCE

Secure Missions Solutions *a Parsons Company*

- Assessment and Authorization Support for Air Force / Defense Health Agency
- RMF Support for three Army Projects

ProSPhere Tek, Inc.

- HUDOIG Cyber Security Program Support

COMPANY CONTACT

Business POC: Rodney McLeod
Phone: (843) 608-0582
Email: rmcleod@mcleodis.com
Address: 1060 E. Montague Ave, Ste 100
North Charleston, SC 29423
CAGE CODE: 7PAQ7 | DUNS Number: 080320339

NAICS CODES

541512 Computer Systems Design Services
541519 Other Computer Related Services
541513 Computer Facilities Management Services
541690 Other Scientific and Technical Consulting Services

SERVICES

A&A SUPPORT

Our process for Assessment and Authorization (A&A) places initial focus on boundary definitions, definition of roles and responsibilities, and security categorization based upon data types and sensitivity. After conducting a comprehensive risk assessment, our team is able to develop system security plans that explain who, what, how, and how often for each security control (leveraging common or inherited controls where possible). Our teams also develop all supporting documentation, such as eAuthentication Risk Assessments, Privacy Impact Assessments, IT Contingency Plans, Security Control Assessment/Test Plans, Security Assessment Reports, ATO Letters, and agency-

VULNERABILITY SCAN AND REMEDIATION

A vulnerability is a weakness in a system or network that can be exploited by an attacker to gain unauthorized access. An effective vulnerability assessment and remediation program must be able to prevent the exploitation of vulnerabilities by detecting and remediation vulnerabilities in the system or network in a timely fashion. Proactive managing vulnerabilities on covered devices will reduce or eliminate the potential for exploitation and save on the resources otherwise needed to respond to incidents after an exploitation has occurred. Our team has experience in designing, implementing and operating programs to ensure the security of you system or network.

POLICY & PROCESS DEVELOPMENT AND IMPROVEMENT

All companies should develop and maintain clear and robust policies for safeguarding critical business data and sensitive information, protecting their reputation and discouraging inappropriate behavior by employees.

Many of these types of policies already exist for “real world” situations, but may need to be tailored to your organization and updated to reflect the increasing impact of cyberspace on everyday transactions. As with any other business document, cybersecurity policies should follow good design and governance practices -- not so long that they become unusable, not so vague that they become meaningless, and reviewed on a regular basis to ensure that they stay pertinent as your business needs change.

SECURITY CONTROL ASSESSMENT (SCA)

A SCA is the formal evaluation of a system against a defined set of controls. The SCA and ST&E will evaluate the implementation (or planned implementation) of controls as defined in the SSP. The results are the risk assessment report. This report will document the system’s areas of risk

CONTINUOUS MONITORING

Continuous monitoring and assessments at all levels and during the system life-cycle will decrease the overall risk to an organization and ultimately reduce the overall impact from breaches. We implement a six-step process as is indicated in the DHS Continuous Monitoring brochure or as outlined in the NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems, September, 2011.

SECURITY CONSULTING

Our cybersecurity consultants provide services and solutions that deliver continuous security assurance for business, government, and critical infrastructure.