Introduction to ERT

ERT, founded in 1996, is a small, women-owned business enterprise (WBE) that integrates full-spectrum science and technology solutions for federal and state government organizations tackling demanding projects in information technology, Cybersecurity, engineering and science. ERT has been providing professional services to federal government agencies through more than 40 prime contracts. We are certified for ISO 9001:2008 and CMMI Level 2. ERT's information technology services form the essential infrastructure for mission programs across the government. ERT understands that information security is an integral and indispensable part of all business operations that involves ongoing planning, assessment, protection, detection, response, mitigation and training. We provide life cycle IT security services to multiple agencies within NOAA which include National Weather Services (NWS), National Environmental Satellites Data and Information Systems (NESDIS) and National Ocean Service (NOS) Chief Information Officer (CIO). We are responsive and agile, placing high value on effective customer service and technical excellence. Our cost, management and technical performance scores are consistently in the excellent range.

Earth Resources Technology

6100 Frost Place, Suite A, Laurel, Maryland 20707
Point of Contact: Jingli Yang, CEO
301.323.1437 • Fax 301.361.0620
www.ertcorp.com
Contract Number: TIRNO-11-D-00056
Contracting Manager: Kim Lester, 301-323-1439

Introduction to TIPSS-4

The IRS competed its first Management/Business Operations Support Services and Cybersecurity suite of indefinite-delivery, indefinite-quantity contracts, called TIPSS-4 SB, which have a 10-year period of performance (one base-year and nine one-year options) and a program ceiling of $2 billion. These contracts are the primary procurement vehicle for technology-related services within the Internal Revenue Service and other Treasury bureaus.

The TIPSS-4 SB contract is designed to provide a full range of information processing support services for project and program level support and Cybersecurity related services that maybe required across virtually all software languages and hardware platforms throughout the period of performance of the contract.

Available Services:

ERT provides services under the following four functional areas:

- Security Policy and Planning
- Assessment and Authorization
- Security Implementation
- Security Operation, Support, and Training

ERT

TIPSS-4

Total Information Processing Support Services

Cybersecurity

ERT

TIPSS-4 Benefits

- Directed task orders up to $2 billion
- 1-year base period, 9 option years
- IRS and other Treasury bureaus' preferred acquisition vehicle
- Satisfies Small Business requirements
- Multiple contract types with performance-based solutions available
- Streamlined procurement lead times
- One-stop shopping: Full Service Procurement Services
- Access to trusted and reliable small business industry partners
- Proven performance track record

Getting Started

Government Contact for Contract Administration
Ms. Carol Grohman
TIPSS-4 Contracting Officer's Representative (COR)
Desk: 202-283-6910
Email: Carol.B.Grohman@irs.gov

ERT provides the following professional services:

Security Policy and Planning

- Assist in development, review and maintenance of system security plans, policies, procedures, and best practices
- Conduct annual testing of contingency and disaster recovery procedures
- Develop IT security documentation for system security plans, disaster recovery and continuity of operations plans
- Provide expert advice and recommendations based on the National Institutes of Standards and Technology (NIST) Special Publication (SP) 800 series, Federal Information Processing Standards (FIPS), and industry best practices

Assessment and Authorization

- Perform system testing and evaluation to assess the security posture of information technology systems
- Conduct vulnerabilities scans; perform compliance scans
- Assist ISSO to mitigate system risks and remediate vulnerabilities
- Manage the Assessment and Authorization (A&A) process for High and Moderate systems and applications per NIST guidance
- Develop and maintain A&A documentation; review for completeness and compliance with security policies, procedures and guidance
- Develop and track all Plan of Actions and Milestones to ensure that the highest level of security posture is maintained
- Perform independent assessments of security controls for applications and systems

Security Implementation

- Develop, implement, and maintain an IT security program consistent with federal laws, and agency regulations, policies, procedures and standards
- Ensure implementation of all organizational security policies, plans, and procedures
- Design, implement and integrate controls to meet security requirements within the risk management framework
- Evaluate new security technologies and applications, and recommend change options to the information system owner
- Apply robust configuration management and change control processes
- Ensure distribution, tracking and timely implementation of approved security alerts, patches, and bug fixes
- Deliver secure and compliant cloud solutions integrating existing agency architecture with that of service providers

Security Operation, Support and Training

- Provide system monitoring, network intrusion detection, audit logging services and compliance reporting
- Maintain the security baselines for systems; update hardware, patch software, perform backups and restores
- Respond to IT Security incidents including but not limited to intrusions, system compromises, inappropriate user actions, use of peer-to-peer and potentially unwanted programs, detection of malware, spyware, or viruses, and loss or theft of government IT resources
- Investigate security violations, perform computer forensics as needed, and generate detailed reports
- Schedule and coordinate local security training and awareness programs for users; ensure that privileged users receive system-specific training prior to being authorized access to the system; ensure specialized IT security training is available to all system and network administrators