

CYBERSECURITY

SRC combines **operational and technical cyber expertise to defend networks and the critical information** flowing through them

As a trusted and recognized leader for cybersecurity solutions, SRC provides objective recommendations to government and commercial information security officers to ensure mission and business success.

Information is the lifeblood of any organization, and for decades, SRC has helped the U.S. Intelligence Community (IC) define security requirements and implement strategies to secure their enterprise IT infrastructure from sophisticated internal and external attacks.

Through scientific research, extensive education and hands-on experience, our cybersecurity experts have developed solutions and services to help protect networks and the information flowing through them

HIGHLY TRAINED WORKFORCE

Exceptional outcomes are the result of a highly trained workforce, and SRC's personnel are some of the most sought-after experts in the field. We are agile and dynamic, providing



unparalleled service to meet our customers' demands – whether it's a computer security shortfall, or a gap in their governance, risk management, and compliance needs. SRC offers unbiased, credible assessments and recommendations to prioritize the selection and implementation of security controls, compensating controls, protection mechanisms, cybersecurity frameworks or standards.

Our certified information assurance experts have achieved:

- Certified Information Systems Security Professional
- Certified Information Security Manager
- Assessment and Authorization (A&A) Professional
- CompTIA™ Security+
- Global Information Assurance certifications
- Various software and hardware vendor certifications

RISK MANAGEMENT

SRC's information technology security professionals create new solutions to unexpected problems by evaluating threats and mitigating potential risks in real-time. We have been commended for maintaining continuity of essential operations and access to data during attacks.

**AS A TRUSTED ADVISOR
TO OUR CUSTOMERS, WE
PROVIDE ALL-INCLUSIVE
CYBERSECURITY SERVICES**

Our experts are fluent with the following standards and methods:

- DOD and IC implementations of the National Institute of Standards (NIST) and Technology Risk Management Framework
- NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)
- GSA FedRamp
- U.S. Security and Exchange Commission Compliance Procedures
- International Organizations for Standardization (ISO) families including 17020, 27001, 27002
- CIS, COBIT, FERC, FISMA, GLBA, HIPAA, ITAR, NERC, and a multitude of other commercial, national and international standards and directives

CYBERSECURITY

POLICY & PROGRAM PLANNING

Our analysts proactively design customer policies and programs to effectively and reliably share information. Our in-depth knowledge of the principles and practices of cybersecurity is evidenced by our long-standing reputation of quality planning for the IC. We offer the following tailorable planning services:

- Security policy, operational procedure, and organizational policy and processes using standards from the DoD, IC, Office of Management and Budget, National Information Assurance Training Standard and Committee on National Security Systems, and according to international and federal law
- Gap analysis, identification of program needs, and corresponding roadmap recommendations
- Post implementation periodic review, analysis, risk assessment, and more

SECURITY ENGINEERING

SRC's protection engineering expertise has been instrumental in helping assure our customers' systems are safe from attack. We assist our customers in fulfilling vague government requirements by:

- Building security compliance requirements into the system development lifecycle
- Employing multi-discipline engineers that integrate all forms of technologies in order to create a compliant and secure solution
- Performing operational security engineering support of deployed and legacy systems

ASSESSMENTS

Our team is highly skilled in planning and executing assessment and testing services based on third-party standards, such as:

- Proactive assessment that establishes a point-in-time baseline for both technical and non-technical cybersecurity posture. Assessment is tuned to verify and validate major and minor changes to an enterprise or network
- Penetration testing to target known or unknown enterprise vulnerabilities
- Static and dynamic web application testing focusing on both functional and security assessments of currently deployed or pre-production applications
- NIST Risk Management Framework Step 4 assessment services to ensure security control compliance

COMPUTER NETWORK DEFENSE/ OPERATIONS SUPPORT

As a trusted advisor to our customers, we provide all-inclusive security operations and computer network defense services that include:

- Detection and monitoring of security threats, including continuous, round-the-clock event detection, situational awareness, incident management and tracking; and sophisticated forensics and malware analysis
- Custom cyber situational awareness tools to provide real-time detection of malware infection to prevent data loss and beaconing, while supporting real-time intelligence in action



800-724-0451 • inquiries@srcinc.com • www.srcinc.com

Scan QR code to download an electronic copy.

© 2020 SRC, Inc. All rights reserved. 20201203

