Cybersecurity

Cybersecurity and infrastructure vulnerabilities pose a serious threat to our economy and national security. Cambridge leverages our proven experience in incident response, cyber threat intelligence, security engineering, and Assessment and Authorization (A&A) to enhance our customers' capabilities across the DoD and Federal enterprises.

Our Cyber Network Defense (CND) experts can help identify and eliminate threats through Cyber intelligence, traffic monitoring, vulnerability scanning, application scanning, and endpoint protection. Additionally, our compliance cadre have mastered the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and provide full-spectrum A&A services including the development of System Security Plans (SSP), Contingency/Disaster Recovery Plans and audit policy. They also provide Risk Assessment, Security Controls Assessment, and Security Program Review services to ensure compliance with Federal IT Security requirements.

Areas of Support

- Secure Federal Networks
- Protect Critical Infrastructure
- Cyber Incident Response
- Continuous Security Monitoring
- Vulnerability Management
- Insider Threat Detection
- Data Loss Prevention
- Penetration Testing
- Log Management
- Information Assurance

Certification and Accreditation (C&A)

Cambridge offers significant C&A support experience in NIST RMF, Intelligence Community considerations, and Commercial Cloud FedRAMP testing in support of a third-party assessment organization (3PAO). Each C&A event provides our customers a true picture of the security posture of the environment. Most critical, our solutions focus on action, tracking, and demonstrated proof of results. We don't just tell the customer what is wrong, we provide tailored paths to close gaps and demonstrate the effectiveness of the implementation to accreditation officials. Team members hold DoD 8570.1 and other federal credentials.

Incident Response

We provide support to identify potential threats, log and track incidents, provide forensic analysis, and work through the Incident Response process. Our analysts and engineers include personnel with Global Information Assurance Certification (GIAC) and GIAC Certified Incident Handler (GCIH) certifications.

Security Engineering

We provide both hands on and consultative support to assist in the hardening of systems. These efforts are balanced with the mission need and business considerations. We recognize that there is no "one-size-fits-all" set of solutions.

Considerations Include:

- NIST RMF, DISA STIG, or organizational policy requirements
- Data and system protection levels
- Cost, time, quality, risk, and scope
- Specific mission requirements to meet organizations goals
- Effective communication of risk and proposed mitigations or remediations
- Integration with current environment to leverage existing protections

Threat Analytics

Our threat analytics efforts focus on providing data specific to the organization's risk levels. This allows the prioritization of the mitigations and remediations the organization undertakes. This is a growing area of importance and is particularly useful when considering Commercial Cloud implementations in the Federal Government.

Programmatic Support

We provide our customers with accurate financial and scheduling support. The team also helps senior cybersecurity personnel with training, documentation/policy, and programmatic assessments of an organization. Additionally, we play a key role in helping our customers understand what their true cybersecurity posture looks like. Though this can often be initially challenging to accept, the reality is that an accurate portrayal is key to strategy.

Proven Performance

Our custom fit technical approach allows us to provide additional value to our customers by incorporating their specific needs as opposed to "one-size-fits-all" solutions. Our solutions also place a focus on organizational mission and providing solutions that consider business drivers and existing environments. This custom approach provides specific value to customers.

National Aeronautics Space Administration (NASA) Base Information Technology Security(BITSec)

The BITSec task is dedicated solely to the support of the cybersecurity initiatives and operations of the Johnson Space Center (JSC) Information Technology Security Office (ITSO). A broad spectrum of support services are supplied on this contract. These include: Incident Response team; Vulnerability assessment program; Assessment and Authorization; Cyber Threat Analytics; Intrusion Detection and Prevention services; SPLUNK log analysis and recommended actions; Program Management review, policy, and training. Our CPARs demonstrate our value to our customers. In response to our metrics reporting capability our customer says, "This advanced reporting capability resulted in significant security improvements such as a 40% reduction of JSC public-facing vulnerabilities and a 50% reduction in expired Authority to Operate (ATO)."

Naval Engineering Training Command (NETC)

Cambridge subject matter experts (SMEs) provide security engineering, testing, and support of accreditation efforts to our prime, CSRA. This worldwide task involves a diversity of technology to execute. Windows Server, Windows workstations, Linux, Internet Information Server (IIS), MS-SQL, Cisco networking equipment, and more are involved. Cambridge provides support for the Assured Compliance Assessment Solution (ACAS) and Host-Based Security System (HBSS) implementations designed to provide protections to the infrastructure. In a recent case the Cambridge team provided lead SME support resulting in an improvement for a CCRI from 70.7% to 83.3% on NIPRNET and from 31.8% to 77.4% on SIPRNET. This resulted in a 17.8% improvement on NIRPNET and 147% improvement on SIPRNET. This result was provided on a multi-location system with hundreds of systems within a six-week period.

Military Sealift Command (MSC)

Cambridge provides Information Assurance support to MSC including patch, compliance, and risk management. We support ARC accreditation and Risk Management Framework transition activities for the MSC C4 Engineering (MCEL) Lab as well as for Afloat CLAN GOSUP (ACG(V)2), Afloat Release 2 (AR2), and Shipboard Management Information Systems (SMIS).

CAMBRIDGE
INTERNATIONAL SYSTEMS

2300 Clarendon Blvd, Suite 705
Arlington, VA 22201
(571) 319-8900
www.cbridgeinc.com