Agility. Strategy. Insight.

209 Burlington Road, Suite 105
Bedford, MA 01730
Tel: 781-273-1600
Fax: 781-276-3600
www.s4inc.com

Cybersecurity Capabilities

S4 Inc. provides DoD and US Government Customers with Cyber, Network & Information Security

S4 Inc. specializes in helping Department of Defense (DoD) and US Government customers including NORAD and USNORTHCOM (N&NC), USCYBERCOM, USSTRATCOM, USTRANSCOM, DISA, US Air Force, US Army, US Navy and DHS protect their computers, networks and information from cyber threats. The following paragraphs describe our cybersecurity experience.

Cyber Training. For N&NC, S4 provides a training plan for the Cyberspace Warning & Operations Center (CWOC) Computer Network Defense (CND) and Systems and Network Monitoring (S&NM) watch positions. We coordinate, facilitate and schedule training opportunities for: N&NC C4 Planner Course; What's up Gold (WUG); Integrated Tactical Warning/ Attack Assessment (ITW/AA); BMDS; N2C2 and DHS N&NC Network Defense Posture Level; N&NC Joint Cyber Center; CYBERCOM; N&NC C4 Planner Course; DHS; Host Based Security System (HBSS); SSIM and INTRUST.

Cyber Planning & Policy. S4 provides expertise to the N&NC/DHS Cyber Coordinator to ensure information sharing between N&NC, the National Cyber security and Communications Integration Center (NCCIC), and the US Computer Emergency Readiness Team (CERT). This ensures shared awareness of cyber initiatives and potential impacts to Command's Defense Support of Civil Authorities (DSCA) and Homeland Defense (HD) missions and activities. S4 also promotes the information sharing of cyber issues related to cyber support policies, plans and capabilities to facilitate DSCA and HD planning and execution. We provide DoD perspectives to DHS's efforts in cyberspace operations, plans, and exercise implementation for Homeland Security/Homeland Defense and DSCA to determine capability gaps as well as impacts on DoD (N&NC) cyberspace initiatives. S4 furnishes After Action Reviews, After Action Reports, Lessons Learned and Hot-Washes following each exercise and real world event.

Computer Network Defense (CND). S4 supports CND and S&NM for the N&NC CWOC. S4 personnel conduct 24/7/365 monitoring, reporting and analysis for the N&NC Command and Control Systems in support of mission objectives. We also participate in the cyber intelligence and network operations community for the coordination and collaboration of cyber threat analysis representing best practices and tactics, techniques and procedures (TTPs). This community includes national liaison offices and service organizations (i.e., DIA, CIA, NSA, USCYBERCOM, Combatant Commands, and respective service elements associated with the cyber domain).

S4 supported the US Navy Cyber Defense Operations Command (NCDOC) in coordinating, monitoring, and overseeing the defense of the Navy's computer networks and systems of more than 700,000 users. NCDOC is responsible for centrally managed enclaves, legacy systems, and "excepted" networks authorized by the Cyber Asset Reduction and Security Task Force to operate independently. S4 analysts supported research and analysis by screening network logs, and all-source cyber intelligence reporting; assessing and summarizing evaluated and previously unevaluated information collected as part of day-to-day operations; discriminating threat information from all source cyber intelligence; and fusing information into actionable intelligence for dissemination of warnings and threat analysis as appropriate.

CMMI SVC /2 SM
Exp. 2019-05-18 / Appraisal #26810

TÜV MANAGEMENT SERVICE ISO 9001

Agility. Strategy. Insight.

209 Burlington Road, Suite 105
Bedford, MA 01730
Tel: 781-273-1600
Fax: 781-276-3600
www.s4inc.com

Network & Information Security. S4 personnel monitor and report on the security of USSTRATCOM networks by monitoring security Information Assurance Vulnerability Alerts and implementing security procedures, such as firewall administration and virus protection strategies, to protect networks from unauthorized access. S4 has provided Security Incident & Event Management (SIEM) Services, Demilitarized Zone (DMZ) Services, and Malware Detection & Protection (MDP) Services for our customers. We support deployment of tools, provide HBSS engineering and analysis support and Security Incident and event management.

For the N&NC CWOC, S4 analysts perform assessments of Information Assurance Vulnerability Assessment (IAVA) compliance and maintain global situational awareness of IA and CND events. S4 tracks and reports network changes, such as INFOCON; IAVA system; USCYBERCOM and JFHQ-DODIN Tasking Order (TASKORD)/ Warning Order (WARNORD); Fragmented Order (FRAGO) and Operation Order (OPORD) notifications. We provide characterization and assessment of C4 incidents and issues, as well as situational awareness reports, for review and Government acceptance. S4 develops and provides recommended TTPs to improve installation, integration, and employment of new and existing IA/CND and Enterprise Management toolsets. S4 also develops Course of Action (COA) plans to mitigate any potential N&NC degradations. We facilitate assessments and validation of N&NC compliance with IA/CND policy and directives. S4 assists in the coordination with N&NC Information Assurance for active Risk Assessments and Management/Mitigation and Information Assurance initiatives.

Assessment & Authorization. S4 provides technical assessments, risk analysis, mission impact assessments, and recommendations to mitigate any potential N&NC degradations. S4 personnel validate current policy requirements and report non-compliance using the required DoD compliance reporting system. S4 supports the development and integration of operational TTPs internal and external to N&NC; Playbooks; Development of Theater Net-Centric Strategies; NetOps situational awareness operations; and NetOps Concept of Operations (CONOPS). We also conduct analysis of all issues associated with and required for situational awareness of N&NC systems, networks and services.

S4 provided validation support to the US Navy Information Operations Command (NIOC). We facilitated delivery of C&A artifacts such as IATT, IATO, IATC, and ATO documentation to the NCDOC Information Assurance Manager (IAM). S4 responsibilities included C&A of NCDOC systems leveraging current IA controls (DIACAP and FISMA) guidance and methodologies. S4 was responsible for ensuring all efforts met confidentiality, integrity and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems.