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.

Policy Analysis. For the USCYBERCOM Chief Information Officer (CIO), S4 Inc. provides insightful analysis, and critical thinking, of higher level policy initiatives to prepare USCYBERCOM position and response actions to existing and future policy. S4 analyzes current DoD cybersecurity policies, processes, capabilities, authorities, architectures for applicability to USCYBERCOM C4/IT systems, cybersecurity processes, and CIO responsibilities. S4 provides recommendations for generating original, or improving on current, policies, implementation plans, and strategies. S4 participates on enterprise-level and inter-agency boards, panels and working groups which serve as the forums in which DoD C4/IT program policy directives are negotiated and defined. S4 bears continuing responsibility for facilitating in-house SME assessment of proposed policy directives and other agreements. S4 conducts research of the complex issues planned for discussion, and defines proposed Command positions. S4 analyzes and provides expert assessments to leadership of the likely effects of approved policy directives, including possible need for further lobbying and action by the Command and its constituencies, and prepares working papers. We apply expert knowledge of the program and policy landscape to make substantive contributions to the development of executive-level briefings, congressional responses, and other highly-sensitive communications of enterprise-level program intent.

Policy Assistance and Implementation. S4 Inc. provides assistance to USCYBERCOM CIO policy developers through analysis of higher level policy, strategy, and similar policies of other DoD components. S4 reviews higher level policy and assists in the assessment and refinement of USCYBERCOM CIO and cybersecurity policies IAW higher level policy. S4 assesses gaps in existing USCYBERCOM policy and proposes amendments to existing policy or proposes recommendations to address any gaps therein. S4 participates in the implementation of enterprise-level (Command, Service, DoD, or Federal Government-wide) policy directives and other guidance materials. We distribute policy directives throughout the Command, including the supplemental guidance materials essential to ensure affected organizations' understanding of implications for their operations, and full and proper implementation.

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 Inc. 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.

Network & Information Security. S4 Inc. 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.

Risk Management Framework (RMF). S4 Inc serves as the subject matter expert for USSTRATCOM/J64's Risk Management Framework (RMF) overseeing DODI 8510.01 (RMF) activities, assessing systems IAW DODI 8500.2 and CNSSI 1253 and selecting security controls (NIST 800-53). S4 provides RMF support for IT system hardware, software, and network operations supporting the Command and Control Facility (C2F). S4 performs cybersecurity roles and initiates RMF processes for assigned systems. We provide cybersecurity analysis support and recommendations including system-level risk analysis, security control selection and implementation, risk identification, remediation, and mitigation. S4 analyzes plan of action and milestones (POA&M) and provides recommendations on operational cybersecurity issues. We also provide analysis to optimize cybersecurity risk mitigation strategies. S4 analyzes certification evidence and artifacts, conducts risk analysis and prepares recommendations for accreditation decisions.

S4 provides technical assessments, risk analysis, mission impact assessments, and recommendations to mitigate any potential N&NC degradations. S4 validates current policy requirements and reports non-compliance using the required DoD compliance reporting system. S4 helps develop and integrate 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 conduct analysis of all issues associated with and required for situational awareness of N&NC systems, networks and services.