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, Joint Electromagnetic Warfare Center (JEWC), US Air Force, US Army, US Navy, and DHS protect their computers, networks, and information from cyber threats.

Risk Management Framework (RMF). S4 Inc serves as the subject matter expert for USSTRATCOM, USCYBERCOM, and Joint Center for Electromagnetic Readiness (JCER) RMF activities IAW NIST Special Publication 800-37, overseeing DODI 8510.01 requirements, assessing systems IAW DODI 8500.2 and CNSSI 1253 and selecting security controls IAW NIST 800-53. S4 provides RMF support for IT system hardware, software, and network operations supporting USSTRATCOM, USCYBERCOM, and JCER mission areas. 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 experts analyze plans of action and milestones (POA&M) and provide 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 uses the Enterprise Mission Assurance Support Service (eMASS) to support RMF system security package generation and manage all cybersecurity compliance activities and automation of the workflow process from system registration through system decommissioning.

Policy Analysis. For the USCYBERCOM Chief Information Officer (CIO), S4 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, and architectures for applicability to USCYBERCOM C4/IT systems, cybersecurity processes, and CIO responsibilities. S4 experts provide 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. We conduct research of the complex issues planned for discussion, and define 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. supports 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 personnel participate 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.

Defensive Cyber Operations (DCO). S4 Inc. supports DCO for USSTRATCOM, N&NC, and the JEWC by providing continuous monitoring of systems on NIPRNet, SIPRNet, Joint Worldwide Intelligence Communications System (JWICS), and Special Access Program (SAP) networks. For USSTRATCOM, S4 experts report security incidents and threats for systems and networks IAW USSTRATCOM Network Operations Center

(STRATNOC) procedures using cybersecurity tools and resources supporting those activities. We perform security enhancements for software, hardware, physical and logical architectures to reduce vulnerabilities and implement DISA Security Technical Implementation Guides (STIGs) and Information Assurance Vulnerability Alerts (IAVAs). Our team's comprehensive security procedures encompass internet security, firewall administration, virus protection strategies, and protection from unauthorized access. S4 personnel perform reviews of random workstation configurations, server logs, and firewall reports to identify anomalies, alerts, and alarms and promptly forward all findings to appropriate command Information Systems Security Manager's (ISSM's). We perform daily monitoring of email content scans including proper classification markings and report deviations of USSTRATCOM policy and DoD regulations to the STRATNOC.

S4 experts respond to customer inquiries on security related topics such as spam, viruses, malware, possible malicious sites, website blocks, host issues, and traffic dropped by security tools. We analyze incident tickets and perform threat analyses of websites, troubleshoot email issues, and update security tools on clients. S4 personnel troubleshoot connectivity performance and issues that may be caused by network security tools. We perform equipment and software management to ensure latest versions are installed and configured. S4 handles all intrusion prevention and detection, log correlation and review, email content scanning, intelligence report review, and network anomaly detection services. These services support CDR USSTRATCOM's connectivity with Nuclear Command, Control, and Communications (NC3) assets and provide overall situational awareness.

S4 performs DCO for N&NC systems and networks and acts as a liaison with other N&NC cyber operations centers including the Cyberspace Warning and Operations Center (CWOC) and the Joint Cyber Center (JCC). We enforce network cybersecurity policies; support operation of network sensors; monitor and analyze network behavior; perform network tuning/optimization; and implement network cybersecurity countermeasures. S4 initiates network boundary management and control activities; maintains network access and security; analyzes cyber vulnerabilities; and initiates appropriate responses. S4 experts ensure all network and service monitoring tools are configured, optimized, and tuned to enable proactive network monitoring and network defense.

S4 CWOC analysts support N&NC DCO by performing assessments of cybersecurity compliance and maintaining global situational awareness of cybersecurity events. S4 tracks and reports network changes, such as Information Operations Condition (INFOCON); 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 cybersecurity 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 cybersecurity policy and directives.

S4 supports the JEWC by assisting the Information System Security Officer (ISSO) with network security incident response and management. S4 experts report network security incidents such as a violation or imminent threat of violation of computer/network security policies, acceptable use policies, or standard security practices. We work diligently to discover violations and effectively contain the damage; eradicate the violations presence; and restore the integrity of the network and systems. S4 collects and analyzes data related to any widespread system or service outage; and we document and disseminate system technical data ensuring DoD and Government regulatory compliance. We evaluate trouble tickets for JEWC National Security Systems and perform technical tasks to resolve software and hardware cybersecurity issues. S4 experts prepare draft and final evaluation reports on the cybersecurity issues, including an executive summary; an assessment of mission impact of the noted problems; a listing of all documented problems; and recommendations for system corrections and/or improvements.