Security Engineering and Management
U.S. Marine Corps
Past Performance

As part of G2SF's Operations and Maintenance Contract in support of the Marines, G2SF is tasked with providing security requirements identification, analysis, allocation, and tracking support utilizing the Risk Management Framework (RMF). These efforts also include assisting the Government in retaining the Authority to Operate (ATO) through all software upgrades and capability improvements as well as developing and editing accreditation packages for the training, pre-production, and production environments. In support of these requirements, G2SF System Engineers and IA specialists create and maintain Plan of Actions and Milestones (POAMs) for five (5) environments and remediate or mitigate findings discovered during Assured Compliance Assessment Solution (ACAS) and Security Content Automation Protocol (SCAP) scans. G2SF ensures adherence to all DOD and USMC standards and regulations while providing documentation and information needed to obtain, maintain, and re-certify the systems ATO. G2SF assists in answering data calls as packages progress through the Risk Management Framework (RMF) processes during the system upgrades. G2SF engineers continually build and harden operating systems and applications during upgrades and installations by applying appropriate Security Technical Implementation Guidelines (STIG's) and resolve STIG conflicts as well as maintain security posture by ensuring that scheduled patching of systems and applications are completed on time. G2SF IA engineers also work with the Information System Security Officers (ISSO) to respond to requests for information and security directives.

G2SF developed a Vulnerability Management Plan (VMP) based on the 7-step Risk Management Framework. The VMP supports the mitigation of security issues and incidents that introduce security risks. The VMP documents the roles and responsibilities that relate to performing security scans, reviewing and documenting results in a POA&M, resolving or mitigating identified issues, and updating the ATO package appropriately. These efforts are coordinated between G2SF, Government IA staff, Network Situational Awareness Common Operational Picture (NetCOP), and Marine Corps Enterprise Information Technology Services (MCEITS). Our VMP-driven processes have proven highly successful in supporting USMC IA efforts to protect the confidentiality, integrity, and availability of online information, systems, networks, and services.