

Technical Support for Medicare Contractors Security Assessment and Planning Description

Northrop Grumman provides security gap analysis for Federal Information Security Management Act (FISMA) reporting and helps identify costs and track and correct weaknesses for the Centers for Medicare & Medicaid Services (CMS) through the testing and audit finding remediation of Medicare contractors (business partners) and CMS internal systems. Business partners include those covering Part A, Part B, Data Centers, Coordination of Benefits (COB), Program Safeguard Contractor (PSC) and Durable Medical Equipment Regional Carrier (DMERC) entities. CMS is currently rolling out this process enterprisewide for use on all remaining CMS systems.

Issues are tracked against the Northrop Grumman-developed CMS Core Security Requirements (CSRs) based on FISMA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Privacy Act, and other Federal security requirements as benchmarks for CMS security. These CSRs are incorporated in the CMS Integrated Security Suite (CISS). CMS business partners and business owners use the CISS to conduct cost-effective, consistent and accurate assessments of the IT systems and to track weakness remediation efforts for the Plan of Action and Milestones (POA&M) reporting required by FISMA. CMS also uses this annual testing and POA&M data records to develop an enterprisewide picture of Medicare systems security, to develop priorities and to identify and track weaknesses for FISMA reporting. The system also allows CMS' budgets for individual business partners to be readily tailored and tracked as needed based on changing Federal priorities and guidance.

Within our process, each identified security gap can be related to a specific relative risk and associated with the criticality of the individual business activity. CMS and Northrop Grumman uses this single database to organize and view the information as it relates to NIST 800-53/53A, HIPAA, FISCAM, FISMA, or any combination of applicable requirements and standards categories.

In addition, the superior security analysis process incorporated in CISS simplifies related Certification and Accreditation documentation, including risk assessments, system security plans, continuity of operations plans, as well as corresponding GAO funding requirements documentation.

Thus, CMS is now able to develop an improved remediation management process targeted at providing the maximum return on investment on an enterprisewide level. The Northrop Grumman-developed CSRs and CISS tools are now staples in the CMS external business partner and CMS internal POA&M tracking programs. These tools, in addition to the CMS/Business Partner Systems Security Manual we developed, have resulted in dramatic improvements in the overall CMS gap remediation process. CMS has reaped immediate benefits in their budgeting process by identifying and disposing of high-risk and/or high-criticality security gaps.