Cybersecurity & Information Technology Torch uses industry and DoD best practices and processes to help provide DoD with Information System Security Management (ISSM), Security Control Assessor (SCA) support and Computer Network Defense. Torch prepares for and conducts Vulnerability Assessments, data analysis, risk assessments, and Risk Management Framework (RMF) reports. The reports are used to support connection decisions such as; Authorization to Operate (ATO), Authorization to Connect (ATC), and Interim Authorization to Test (IATT). Data from tests and authorization decisions are collected, organized, stored, and shared using DoD standard tools such as Assured Compliance Assessment Solution (ACAS), enterprise Mission Assurance Support System (eMASS) and an enhanced Enterprise SharePoint solution. Software Assurance Software Assurance Assurance Implementation of Secure Software Development best practices with static and dynamic code analysis tools, such as Micro Focus Fortify Static Code Analyzer and WebInspect, to detect vulnerabilities in the code and provide actionable remediation strategies. Network Defense & Intrusion Detection Network Defense & Intrusion Detection Network Defense Torch provides Computer Network Defense (CND) at both the Local Control Center (LCC) and the Computer Service Provider (CSP) tiers of responsibility. Torch personnel routinely work all stages of Incident Response (IR), Cyber Tasking Orders (CTO), and Information Assurance Vulnerability Management (IAVM). Risk Management Framework Risk Management Framework Risk Management Implementation, administration, support, and management of legacy DIACAP and RMF requirements; along with other federal cyber security compliance mandates such as Federal Information Security Management Act of 2002 (FISMA), Federal Information Processing Standards (FIPS) Publications, National Institute of Standards and Technology (NIST) Special Publications (800 Series), DoD Instruction 8500.01 and 8510.01. Cloud Security Cloud Security Security Torch teams assist in providing data classification, data security strategy, data management, and data loss prevention using cloud security best practices. Torch Provides Network Security within Complex Systems Network Security within Complex Systems Torch provides IT solutions for data management and computer applications. Torch personnel have database development, web application programming, and enterprise software development experience. We perform design and requirements analysis, implementation, quality assurance, training, documentation, and deployment. This experience is used to develop and maintain data warehouses, enterprise reporting systems, data analysis tools, and management information systems. We also develop and support enterprise-wide information systems to include designing, developing, installing, modifying, and maintaining computer hardware, software, and associated peripherals and licensing agreements. We manage routine upgrades, system security scans and configuration, security accreditation, and disaster recovery programs. Torch is also responsible for network support for classified and unclassified systems. High Performance & Classified Computing High Performance & Classified Computing High Performance & Classified Computing Engineering design of multiple secure large computer clusters and their associated networks, in addition to implementing them into classified environments and providing life cycle maintenance for the clusters. Data Management Data Management Data Management Local and enterprise database and tool development for managing test resources; test results from live, constructive, and virtual engagements; and simulation configurations and results.