COLSA

Cyber & Information Warfare

CYBER SECURITY STRATEGIES TO HANDLE SECURITY IN THE AGE OF CYBER

Every organization faces its own set of challenges, from rules and regulations to highly sophisticated data security threats. Regardless of the size of your organization, one-on-one counsel from a dedicated cyber security engineer is often essential to keep pace. Still short of hiring a dedicated CTO, it can be challenging to pinpoint hidden vulnerabilities, draft the right action plan, or choose the best technologies for your environment to safeguard data assets and comply with new laws—particularly within our fast-paced and ever-adapting threat landscape.

A HOLISTIC APPROACH STARTING WITH COMPLIANCE

Work with a team of professionals who can advise the system owner and organization on the design procedures that adhere to the latest laws, industry standards, and government regulations. We help clients assess their risk versus controls to comply with RMF/NIST.

In addition, our team will work with your cyber security professionals and system owner to develop a holistic plan to go beyond compliance to identify vulnerabilities in software. COLSA's Software Assurance team uses a variety of tools and processes that identify weaknesses in coding even when source code is unavailable. We will identify open source libraries embedded in the code and compare them again the National Vulnerability Database and work with your team to mitigate potential risks.

CYBER SECURITY IS CONTINUOUS

An Authorization to Operate (ATO) only implies the system is "good enough" at that very moment. A steady battle rhythm of network and software hygiene through patches and maintenance combined with independent assessments are the keys to maintaining a secure system. COLSA's team of Cyber Security Professionals are embedded in a multitude of weapons' systems through DoD to ensure proper day-to-day hygiene of the network In addition, COLSA has a wealth of expertise with Blue Teams for cooperative penetration assessments to identify vulnerabilities throughout the system, Green Teams to help fix those vulnerabilities, and Red Teams to independently test the system.

UNDERSTANDING THE THREAT

COLSA's Cyber Security/Information Warfare Team stays abreast of the latest threat from hacktivists to nation states through conferences, continuing education, and formal degreed programs. COLSA's team consists of the "best and brightest" in the industry that includes PhDs, OSCPs, OSCEs, as well as a variety of IAT/IAM Level III qualified personnel. COLSA's team will bring the latest intelligence across the industry to advise the system owner on the desired cyber security posture to best balance security and convenience.