

# Secure(it)<sup>™</sup>

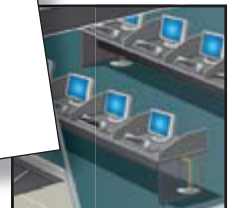
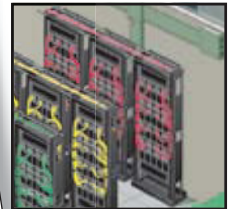
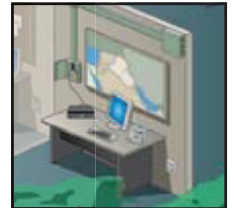
To: US Government Agencies & Departments  
From: CSC Government Team  
Re: Information Assurance & Network Security

Secure and high assurance networks are becoming increasingly prominent across both the commercial and government IT sector. However, specific to government and military applications, the cost of compromise can have dire consequences to the national security and military operations of the United States. Created by National Security Directive No. 42, the Committee on National Security Systems (CNSS) is the designated authority for developing national policies applicable to the security of national security telecommunications and information systems.

In order to increase the security and protection of critical information systems, CNSS advises U.S. Government departments and agencies to implement a multi-layered, multi-vendor approach to security such as a defense-in-depth solution. Part of this strategy includes using multiple layers of technologies or tools to monitor or defend the networks, and acquiring products and technologies from a diverse group of vendors. From a technology perspective, combining a multi-layered security approach including new products and technologies, offers the best protection from potential threats because it requires the attacker to breach multiple layers of security before successfully gaining access to critical system resources.

While utilizing a multi-layered approach does encourage the use of new and emerging products and technologies, government agencies and departments must assume responsibility for understanding the strengths and potential vulnerabilities of any new product or technology as it relates to information assurance and the security of their critical information systems. IA-enabled IT products are required evaluation/validation by NIST or an accredited lab prior to their installation into a secure information system. However, in general, there are not similar standards or specific evaluation criteria established for physical layer or structured cabling products or solutions.

Rather than being certified or validated, most physical layer products designed for secure network applications are reviewed on a deployment-by-deployment basis – especially since the approval is co-dependent upon other facility security aspects (i.e. access control, perimeter distance, information classification, threat level, etc.). Therefore, any vendor promoting their physical layer product(s) as ‘Certified’ or claiming wide-scale approval should be dealt with a great deal of circumspection. Any questions regarding new products or technologies that are being considered for a specific deployment should be directed to the specific Designated Approval Authority (DAA), Information Assurance Manager (IAM), and/or the Certified TEMPEST Technical Authority (CTTA) or Approval Authority (CTAA) PRIOR TO any purchasing activity or infrastructure deployment. This coordination is absolutely critical to minimize potential vulnerabilities to secure information systems and ensure product is not installed that will prolong or prevent the certification and accreditation process.



As part of the Secure(it) initiative, CSC has established and maintained an open dialogue with numerous DAAs and CTTA/CTAAs. By leveraging these relationships, CSC can help end users reduce risk and streamline the review and approval process for their specific network deployment. In addition, CSC can help enhance the security of critical networks by developing a multi-layered approach involving the deployment of new physical layer products and solutions designed to (1) reduce deployment cost and complexity, and (2) enhance network security and defense

**Your information**

**is only as SAFE**

**as your NETWORK**

**INFRASTRUCTURE**