COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) FREQUENTLY ASKED QUESTIONS (Technical)

Last Update: 04 June 2012

Security Requirements

Question: Why are you requiring virtual machines within a Tablet/Laptop solution but not in a Smartphone Secure VoIP solution?

Response: The Tablet/Laptop (Mobility Wi-Fi) Pilot solution provides wireless data capabilities to a SCI enterprise which is being used to develop the Wi-Fi Capability Package so the final requirements may be very different than what was actually deployed. If virtualization technology was commonly available in the Smartphone, we could leverage it for some solutions. To date, the devices that have been considered did not offer that technology. The Secure VoIP solution provides VoIP services to a constrained classified collateral environment. Each solution required a separate risk decision to be made depending on mission; however, the intent is to deploy the best security solutions that are available at this time, document the risk and present it to the accreditors and mission managers. Solutions that do not offer virtualization are not prohibited, but they may be more restricted OR higher risk than ones with virtualization.

Question: What are the requirements for reporting changes *in a "certified"* product including software/hardware baseline changes and changes in manufacturing or suppliers?

Response: CSfC does not certify products, but does approve products for use in CSfC solutions via a protection profile/NIAP and Memorandum of Agreement (MOA). The requirements for reporting changes are contained within an MOA agreed to by NSA and the vendor, so criteria may vary. The MOA states that in the event the vendor independently discovers a vulnerability or makes changes to a product that may potentially cause it not to meet NSA security requirements based on NTISSP No. 11, the vendor agrees it will notify NSA in writing as soon as practicable, of the vulnerability or changes.

Question: How will vulnerabilities identified with COTS fielded products be managed?

Response: This is a process that is still under development. Based upon products in canisters, NSA/IAD can provide guidance on significant vulnerabilities found within those products. Other processes will also need to be deployed such as responding to Information Assurance Vulnerability Assessments (IAVAs).

Question: *What are the approved security "layers"* (protocols and or clarification to COTS protocol options)?

Response: The foundation of Cryptographic Interoperability Strategy is Suite B cryptography. Suite B algorithms are approved by the National Institute of Standards and Technology (NIST). Suite B includes cryptographic algorithms for confidentiality, key exchange, digital signature, and hashing. Specific protocols are in the Capability Packages.

Question: Are all layers end to end? (Red, black, or grey gateways, authentication) Consider three classified enclaves of computers, A, B and C, where A is connected to B with a Site-to-Site VPN solution (basically, two VPN gateways in series), and B is connected to C with a HAIPE solution. Is data sent from A to C encrypted end-to-end?

Response: Not all layers are end to end. In the example above, data sent from A to C would not be encrypted end-to-end. There is a Red gateway at B for traffic between A and C. Each VPN tunnel could authenticate its "peer," however in this example it doesn't yield true end-to-end authentication.

Infrastructure/Enterprise

Question: Are there plans for standard device management?

Response: Yes. Mobile Device Management is a critical aspect for implementing a secure architecture. Capability Packages will ultimately provide direction on how to manage/protect/defend devices.

Device Requirements

Question: What are the physical security requirements?

Response: This is a generic question that can only be answered within the environmental context and policies of a desired capability. Physical security requirements (anti-tamper, tempest, authentication, and display the far end identity) will be documented in Capability Packages and Protection Profiles as required. Additionally, physical control of the device will be covered in a security CONOPS that will describe user and administrative responsibilities for "physically controlling devices and systems.

For more information on CSfC, please see the Non-Technical Frequently Asked Questions.