COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) FREQUENTLY ASKED QUESTIONS (Non-technical)

Last Update: 04 June 2012

GENERAL INFORMATION

Question: What is CSfC?

Response: The National Security Agency's (NSA) Commercial Solutions for Classified (CSfC) Program has been established to enable commercial products to be used in layered solutions protecting classified National Security System (NSS) data. This will provide the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years. It provides customers with an alternative approach for protecting classified information/systems.

Question: Why is NSA changing how it does business from developing and approving specific products for classified customers to creating solutions based on commercial standards and practices whenever possible?

Response: U.S. Government customers increasingly require immediate use of the market's most modern commercial hardware and software technologies within National Security Systems (NSS) in order to achieve mission objectives. Consequently, the NSA Information Assurance Directorate (IAD) is developing new ways to use emerging technologies to deliver more timely IA solutions for rapidly evolving customer requirements. Although NSA's strategy for protecting classified information continues to employ both commercially-based and traditional Government-Off-The-Shelf (GOTS) solutions, IAD will look first to commercial technology and commercial solutions in helping customers meet their needs for protecting classified information while continuing to support customers with existing GOTS solutions or needs that can only be met via GOTS.

Question: How does CSfC differ from the traditional way classified communications devices are procured and provided?

Response: In the past, NSA gathered requirements from customers and then, after the vendor was under contract, a unique solution was built. That process often took four to five years to deliver a "government only product into the hands of the users. Today, instead of building government owned and operated solutions, whenever possible, NSA is moving to a defense-in-depth approach using properly configured, layered solutions to provide adequate protection of classified data for a variety of different capabilities.

Question: How will the certification and accreditation process change?

Response: Customers implementing CSfC solutions will be required to provide evidence to their Designated Approving Official (DAO) that the Capability Package was implemented properly. This evidence would typically include: low-level architectural diagrams with specific products identified; security test results (including evidence the products are properly configured); and evidence that the concept of operations is being followed.

Question: How will NSA make this transition?

Response: CSfC is an option for customers who are interested in quickly deploying cutting-edge technology. Capability Packages will be developed based primarily on customer requirements. IAD is building technical communities internally to support these new roles.

Question: What happens to current GOTS products? Will they be supported by NSA; will they need to transition to CSfC and how long will this take?

Response: In the short term, GOTS products will not be directly impacted by CSfC; however, over time, commercially-based solutions will be integrated into customer's existing infrastructures to provide greater access to the rich set of services in commercial product offerings. The speed of that integration will be driven by the customer. As a result, the balance of deployed solutions will shift from traditional products to more commercial offerings as customers modernize existing infrastructures.

NSA will decide on a case-by-case basis which products will continue to be supported, and the duration of that support. The NSA Client Relationship Management Office will work closely with customers to ensure critical mission capabilities are not impacted.

Question: Who will be responsible and accountable for approving solutions, developing solutions, and implementing solutions?

Response: NSA will be responsible for creating Capability Packages that describe CSfC approved solutions. NIAP will be responsible for approving vendor products through the Common Criteria process, and then NSA will be responsible for listing the products into CSfC canisters, which represent key technology areas used in commercial solutions (i.e., VPN

Gateway, VPN Client, SIP Server, SVoIP Client, etc.), after the vendor agrees to the terms in the MOA. CSfC canisters contain the approved commercial components that are eligible for use in a CSfC solution. Customers will be responsible for implementing solutions that comply with a Capability Package. A customer's DAO accredits the system and decides whether to accept residual risks NSA specifies in the Capability Package. Implementing solutions is the responsibility of the customer or its integrator. Industry develops commercial components that will be used to compose a CSfC solution. Additional details can be found in the CSfC Process section of this FAQ.

Question: Who will be responsible for interoperability among systems, and will there be interoperability Capability Packages or Protection Profiles?

Response: The customer will be responsible for ensuring solutions it procures satisfy its interoperability needs. Protection Profiles are important to CSfC, as they reflect the basic requirements a product must meet to be considered for use in a CSfC composed, layered solution. Interoperability requirements and potential testing will be documented in the appropriate Protection Profiles and/or Capability Package. It is the vendor's responsibility to correctly implement the commercial standards that are referenced in the Protection Profile in order to enable interoperability with Suite B products from other vendors.

CSfC PROCESS

Question: *What is NSA's role in CSfC?*

Response: NSA's primary role is to develop, approve, and maintain CSfC Capability Packages, support solution registration, and maintain a list of CSfC components for solution implementation.

Question: Can you describe the CSfC process?

Response: NSA/NIAP develops Protection Profiles and publishes them to provide customers or vendors with requirements for products so that those products can be used in composed, layered solutions to protect classified information/systems. Vendors have their products independently validated against a Protection Profile(s) by a NIAP Common Criteria lab, and validated under NIST's FIPS 140-2, Security Requirements for Cryptographic Modules, as appropriate. Vendors establish an MOA with NSA. Products determined by NSA to be eligible as components of a solution are listed on the CSfC Components List, available at the unclassified nsa.gov web site. The target audience for Protection Profiles includes commercial product vendors.

NSA develops Capability Packages and publishes them on the unclassified nsa.gov web site. Capability Packages contain information such as a solution architecture, rules for selecting products from the CSfC Components List, non-vendor-specific configuration requirements,

requirements for site testing, rules for using/maintaining/protecting/disposing of solutions, an assessment of the residual risks DAOs must accept when deciding to use a solution, and other pertinent information. The target audience for a Capability Package includes customers with a need for a capability as defined in the capability package (for example, a secure VPN to tunnel classified information between two sites via the Internet), solution/system integrators, and decision makers (such as DAOs, data owners, system owners, etc).

Customers will check the CSfC Capability Packages published on the unclassified nsa.gov web site. If an existing capabilities package meets the customer's needs, the customer will implement a solution that is compliant with the Package. It is expected that customers or their integrators would be capable of implementing a solution compliant with the Capability Package. The DAO at the customer's site will be responsible for accrediting that the CSfC Capability Package was correctly implemented and they are willing to accept any residual risk. It is expected that a customer or their CSfC integrator will provide the DAO with test results and Risk Assessment findings to support their decision to Approve to Operate (ATO). The DAO decides what is necessary to issue that approval.

For information or assistance in determining whether an approved Capability Package satisfies their requirements, U.S. Government customers (e.g., Department of Defense Components, Intelligence Community Organizations, and Federal Agencies) may engage NSA/CSS through their designated IAD Client Advocates. Commercial integrators should coordinate through their U.S. Government customer.

In addition to the traditional system accreditation/approval, a customer must register its CSfC solution with NSA and receive an approval letter. Customers must annually ascertain that their CSFS solution is compliant with the latest version of the Capability Package, and annually re-register the CSfC solution. As needed, NSA will issue alerts to registered customers with solutions. For example, a newly discovered vulnerability in product X might result in NSA sending an alert to customers using product X in their solution to ensure they are aware of the increased risk that will exist until the product is patched, or perhaps to mitigate the risk by making a small change in the configuration of product X.

Question: What is a Capability Package?

Response: A Capability Package contains vendor-neutral information that will allow customers/integrators to successfully implement their own solutions. Using the information in a Capability Package, customers/integrators make product selections while following the guidelines/restrictions to create an architecture with specific commercial products configured in a particular manner. Capability Packages contain architectural diagrams for all critical components for a particular capability (e.g., Multi-Site Virtual Private Network). Capability Packages will have descriptions of the role each component plays for security, either in protecting the mission or putting it at risk, and will identify the approved commercial components that are eligible for use in CSfC solutions. Capability Packages include: a solution's general architecture; list of eligible products; security roles of the products; and requirements for customers, administrators, testers, certifiers/accreditors, key management and lifecycle maintenance. The Capability Package's Risk Assessment will clearly explain the risks being taken. Additionally, guidance documents will outline how components are to be configured and administered.

Question: How will the Capability Packages be developed, approved and updated?

Response: CSfC Capability Packages are approved to protect classified information by the NSA Information Assurance Director. The DAO will decide whether to accept the risk as described in the Risk Assessment for their specific environment.

After a Capability Package is written, for the first implementation, NSA will assist the customer and ensure that all of the necessary information is included. Capability Packages are living documents and will be updated to keep pace with technology and policies as they change over time, as additional security products and services are developed, and as lessons learned from early adopters of this architecture are applied.

Question: How will the component parts be approved?

Response: Vendors who wish to have their products eligible to become CSfC components of a composed, layered IA solution must build their products in accordance with the applicable U.S. Government Protection Profile(s) and submit their products to a NIAP lab using the Common Criteria process. Then, the vendor and NSA enter into an MOA agreement which may stipulate other requirements for the particular technology. Once the product has met these requirements, NSA will add it to the list of commercial products available for use in CSfC.

Question: What is the *customer's role in CSfC? What responsibilities will customers have in* stating their requirements and managing their own security solutions?

Response: Customers will retain full responsibility for stating their requirements and managing their own security solutions based on existing Capability Packages. CSfC Capability Packages will be developed for operational needs considered to be common across the customer community. NSA will work with customers to identify requirements for new Capability Packages.

Question: What is a CSfC canister?

Response: CSfC canisters represent key technology areas used in commercial solutions (i.e., VPN Gateway, VPN Client, SIP Server, SVoIP Client, etc.). They contain the approved commercial components that are eligible for use in a CSfC solution. These are products which meet the requirements of NSA-approved PPs and have been verified by vendor-funded NIAP testing, and further qualified for use in CSfC solutions by the vendors signing an MOA with NSA.

Question: How often will Capabilities Packages be changed and what will vendors and government users need to do ensure they meet standards? What happens if this is too expensive? Will NSA require the vendor or customer to report changes to solutions they are implementing?

Response: CSfC Capability Packages will be reviewed by NSA semi-annually and updated as appropriate. Updates will often be driven by changes in customer needs, technology advances, policies, and problems encountered with use of existing documents. If an integrator/customer decides to make changes to a customer's solution implementation that results in the solution no longer conforming to the CSfC Capability Package, the customer is expected to notify NSA. NSA will review the changes and determine if updates are needed to the documentation. NSA does not control the cost of the solution.

Question: How will changes to Capabilities Packages and Protection Profiles be managed? Describe the process.

Response: NSA will retain responsibility for reviewing requests for changes to CSfC-related documents, identifying the need for the changes, and determining which changes will be implemented. Protection Profiles are developed by industry and government consortia, and maintained by NIAP, and NSA has no plans to change those processes.

Question: Where can I get more information about CSfC, Protection Profiles and Capability Packages?

Response: The unclassified CSfC website is located at http://www.nsa.gov/ia/programs/csfc_program. This site has information outlining the approval and implementation processes for Capability Packages. Updates will be posted to this site as CSfC processes mature.

For general queries about CSfC, email csfc@nsa.gov.

For a current listing of NIAP approved U.S. Government Protection Profiles, go to http://www.niap-ccevs.org/pp/.

For a listing of U.S. Government Protection Profiles currently in development, go to http://www.niap-ccevs.org/pp/draft_pps/.

Additional information about NIAP and the Common Criteria Evaluation and Validation Scheme can be found at http://www.niap-ccevs.org/.

For current Capability Packages, go to http://www.nsa.gov/ia/programs/csfc_program.