ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Utilizing the NSA's CSfC Process

Protecting National Security Systems with Commercial Layered Solutions

Authors

James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

Contributors

Stacey Winn (Fellow – Institute for Critical Infrastructure Technology)

Brian Zielke (Principal Cyber Engineer – ForcePoint)

Underwritten by:

FORCEPOINT POWERED BY Raytheon

Table of Contents

The acceleration of State Sponsored and Mercenary APT cyber-attacks, each of which possess new and more innovative layering of stealth and sophistication, has triggered a much needed response by the National Security Agency's (NSA) Information Assurance Directorate (IAD). A more expedient path to technology approval has been introduced for qualified organizations. As a result, the NSA's IAD is seeking vendor solutions to improve the national cyber-posture through the creation of a comprehensive and timely process and the establishment of the Commercial Solutions for Classified (CSfC) program.

CSfC serves to strengthen the national cyber-posture by enabling commercial solutions to be used in the layered solutions that protect National Security Systems (NSS) information. It set an Information Assurance (IA) requirement consisting of permitted architectures, component criteria, and configuration requirements for vendor solutions to meet. CSfC is designed to provide agencies with a list of components vetted against a common framework that satisfies NSA IAD's security requirements while incorporating emerging technologies and improving national security. The initiative focuses on providing agencies and integrators with options that enable them to design secure data transmission and storage methods and to implement layered security in a timely manner.

Traditionally, the NSA designed and certified U.S. Government systems according to strict design and implementation criteria to ensure the confidentiality, availability, and integrity of sensitive and classified data. Thanks to this rigorous process, agencies could trust that their data was protected and their systems were secure. However, the lengthy time necessary to oversee the creation of systems using the rigorous certification, evaluation, and testing process resulted in systems that were not aligned with the latest cybersecurity trends or current threat landscape by the time they escaped development. Rather than relinquishing the process altogether, the NSA is adapting their strategy. NSA-certified Type-1 solutions, referred to as Government-Off-The-Shelf (GOTS) systems, remain unaffected by the CSfC initiative. Type-2 systems, created according to the CSfC process, utilize Commercial-Off-The-Shelf (COTS) solutions to better meet customer needs in a timely manner. With the right implementation, vendor solutions can be configured and combined to provide robust protection of data when it is stored, processed, or transmitted.

CSfC solutions are composed of available commercial technology that uses open commercial standards. The CSfC initiative is built on three "pillars." First, the National Information Assurance Partnership (NIAP) evaluates and certifies submitted components for inclusion in CSfC solutions. Next, each security function must be layered to provide at least two independent protective capabilities. Finally, CSfC solutions use components such as Suite B

algorithms to ensure confidentiality and interoperability. The process aims to reduce the time to certify secure architecture and devices from years to months or weeks, in order to remain current and technologically aligned. This is possible because CSfC solutions must be composed entirely of widely available commercial technology and standards. This presents a significant cultural shift for agencies and integrators, who need to adjust to the idea that commercial technology can be rapidly adopted for use within tightly controlled national security environments.

Benefits of the CSfC Model

In the past, the government has relied on government designed and certified devices to secure national systems and protect its most sensitive data. The reliance on Government-Off-The-Shelf (GOTS) solutions was due to the extremely high level of control and assurance afforded by individually designed solutions. GOTS went through a strict design and implementation process, with a long, exhaustive security evaluation, so that the end-product had security specific to its design and function.

The main failing of GOTS solutions is that they are inflexible to change and interoperability. As they age, the systems become more difficult and costlier to secure. Lifecycle costs are high and the development cycle is slow. The strict and exhaustive development and approval process slows the introduction of new technology to months or years. Consequently, GOTS solutions rarely, if ever, feature relevant or cutting-edge technology. Instead, they rely on solutions that have proven themselves resilient or secure over time.

Commercial-Off-The-Shelf (COTS) solutions provide a much-needed balance between the security and flexibility needs of government systems. COTS are quick to market and the development of systems made partially or entirely of commercial solutions is almost as rapid. The technology is current and the lifecycle costs are much lower than GOTS solutions. Commercial solutions are designed to include many features and capabilities that are not feasible in government solutions. The level of system integrity and information assurance varies based on the vendor solution and the product incorporated. The primary limitations on the inclusion of COTS in government systems has been the significant loss of government control of the solutions. Without knowing the quality, stability, and flexibility of the product, the government could not ascertain the level of security and assurance offered by the solution. The CSfC program institutes an expedited, but comprehensive, approval, accountability, and implementation process for commercial solutions, so that government systems can have the

increased flexibility, increased utility and lower lifecycle costs of commercial solutions without sacrificing security or stability.

Solutions built within the CSfC framework must pass through an expedited approval process. This could take weeks or months, but it is still significantly shorter than the GOTS process, which has allegedly taken anywhere from a year to almost a decade for some proposals. Under the CSfC program, as soon as components become available and tested, they can be deployed in solutions as needed, without recursive evaluation. As a result, approved solutions can significantly lower the time needed to implement a solution, the cost of the solution, and the bureaucratic burden imposed by the approval process.

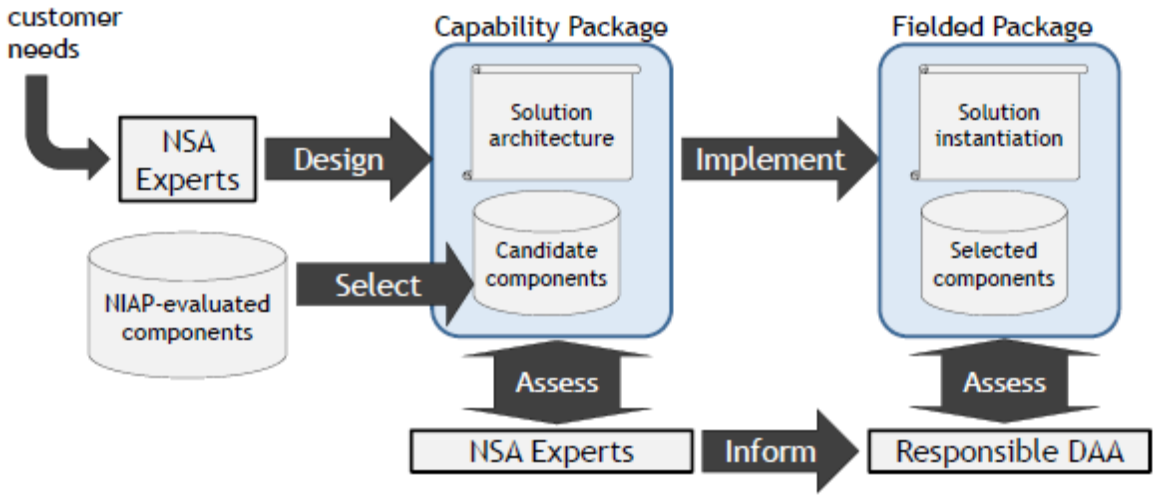
Solutions built using the CSfC Capability Packages can be shared with coalition networks, industry partners, and international partners. Because they rely on commercial products, protocols, and encryption, CSfC products are not Controlled Cryptographic Items. As a result, there is less of a regulatory burden and greater interoperability.

The program engages the Industry to create more relevant, timely, and responsive information systems. Commercial integrators and vendors are incentivized to submit bleeding edge solutions for NIAP evaluation and they are encouraged to incorporate that technology into their solutions. CSfC solutions set an achievable standardized method of meeting regulatory security requirements that would otherwise be unachievable in their environments. CSfC solutions discourage the deployment of unstable or insecure information security solutions that risk national security in their attempt to meet regulatory constraints. Instead, the CSfC initiative allows vendors and product manufacturers to offer the government community the capability of securing their systems, meeting regulatory constraints, and reducing their costs. In short, CSfC solutions improve responsiveness and are designed to precisely and affordably fulfill the customer needs within a reasonable timeframe.

Overview of the NSA Commercial Solutions Strategy

The CSfC process uses composition and independent layers to increase assurance according to customer needs, approved Capability Package, and an expedited approval and implementation process.

The CSfC Process



Source: http://www.rsaconference.com/writable/presentations/file_upload/star-401.pdf.

An agency that has an information assurance requirement will first consult the CSfC Program website to determine if an approved Capability Package exists that meets their requirements. If one exists, they will work with the component developer(s) to build the CSfC solution. The solution is implemented and its independence in the field is assessed. The independence of the chosen candidate components is likewise assessed. Finally, an Authorizing Official (AO) or Designated Approval Authority (DAA) reviews the solution and either suggests changes or assumes responsibility within the bounds of their authority, for the proper operation of the solution.

Capability Packages

CSfC solutions are delivered through Capability Packages, which serve as unique configuration guides for each class of technology. CSfC Capability Packages contain a guideline architecture and description of a CSfC solution: the requirements of component selection, configuration, keying, and testing. They also contain the rules governing the use of a CSfC

solution and its life cycle support; and a classified risk assessment stating the residual risk of the solution.

Capability Packages are intended to accomplish four objectives. First, they provide a guideline for how solutions should be designed, instead of an exact template. Vendors and integrators are permitted, and in some ways encouraged to deviate from the Capability Package. Deviation from the template control introduces cutting-edge solutions into the new systems. The framework is flexible to allow these deviations provided that the solution's assurance level is maintained. Deviations may also be permitted in consideration of implementations in specific environments, effects on the overall mission or purpose, or positive gains to the security of the system. One example of the latter scenario is with Trusted Thin Client® Remote Access. Trusted Thin Client® Remote Access is part of a composed solution that can contain components validated by the CSfC in both the Mobile Access Capability Package and the Data at Rest Capability Package. The Architecture, Component Criteria, and configuration of the solution to meet an Information Assurance requirement are provided by these two packages. Trusted Thin Client® Remote Access is implemented with deviation components that fall within the Mobile Access and Data at Rest Capabilities Packages. With these components applied to the standard Trusted Thin Client® software installation, secure multi-network access is permitted outside of the traditional physical security perimeter without compromising security. System integrators are responsible for ensuring that their specific implementation meets all regulatory and customer requirements specified in the Capability Package and according to the needs of the organization.

Secondly, capability packages provide assurance that a solution will be designed, deployed, and capable of achieving a favorable accreditation decision from the NSA for the protection of classified information. Accreditation is granted based on the NSA's estimation of the mitigation of the risk posed to the protection of classified information through the use of commercial components. Next, the package is consistently updated and evolved according to continuous feedback provided to the NSA. Finally, the Capability Package must provide stakeholders with the necessary documentation to recognize design concerns, usage and environment constraints, necessary components, and assumed risk. Capability Packages are frequently updated to incorporate the latest available technology and to provide updates to integrators and vendors as needed.

Integrators and vendors use Capability Packages to design, build, and deliver NSA-approved solutions according to customer requirements. Because Capability Packages include commercial components and are published by the government, ensuring the approval of

solutions constructed according to Capability Packages are the responsibility of vendors and the government alike. Integrators and vendors allow CSfC components to be implemented into their products based on the specification provided by the NSA. The implementation should be guided and performed by a certified CSfC Integrator, to ensure that the specification is met by the implementation. Capability Packages are used by the AO or DAA to understand how the package addresses customer requirements and to confirm that those requirements are fulfilled. Provided that the integrator or vendor complies with all aspects of the Capability Package, then the AO or DAA can be confident that any CSfC solution is NSA approved.

Pillars of the CSfC Model

Pillar 1: NIAP Certification

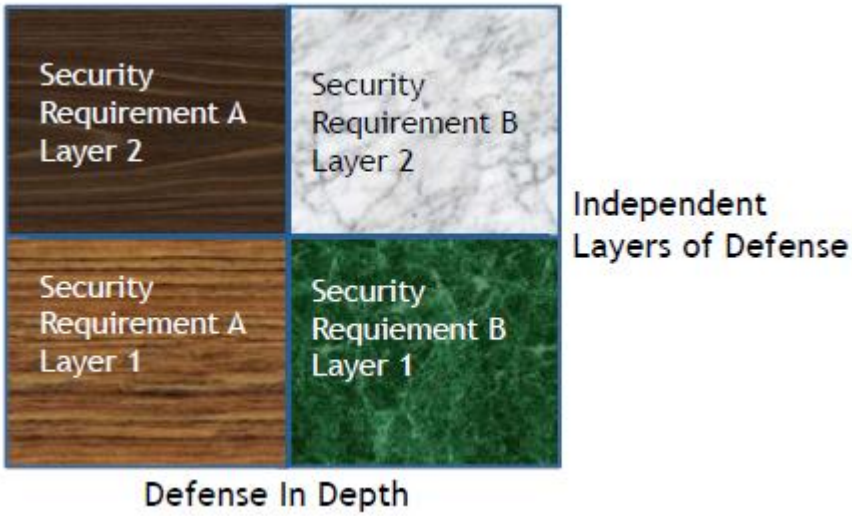
The NSA and National Institute of Science and Technology (NIST) created the NIAP to evaluate the commercial solutions proposed for inclusion in CSfC solutions. The NIAP ensures that commercial products meet NSA standards for security by testing the products against stringent security profiles in certified labs. To be clear, there is not a certification process for either integrators or vendors. Participation in the CSfC program is a process, not a certification. Components are submitted to the NIAP for review, and if approved, the component or mechanism is certified to be included in a Capability Package. Once approved, the commercial products are added to the Approved Products List to be considered by vendors and integrators in their systems under development. A product used in one registration can be re-used easily in similar configurations elsewhere with an easier and, hopefully, quicker journey through registration as long as those components are one of the latest approved CSfC components. When integrators and vendors develop entire systems from Capability Packages and authorized components, the systems will need to be authorized to operate; but again, no certification is needed for the integrator or vendor. The NIAP process is designed to provide consistency and confidence in the ability of commercial devices to secure information, while significantly decreasing the amount of time necessary to design and implement a solution.

Pillar 2: Layered Defenses

The NSA CSfC model is a layered defense information security framework that uses security through composition to increase assurance. Realistically, the strength of the model derives from layers of redundant, trusted components that are supplied by or included in approved commercial solutions. Each information security requirement is supported by

multiple mechanisms. Some mechanisms may support multiple requirements; however, each control remains as independent as possible from other controls.

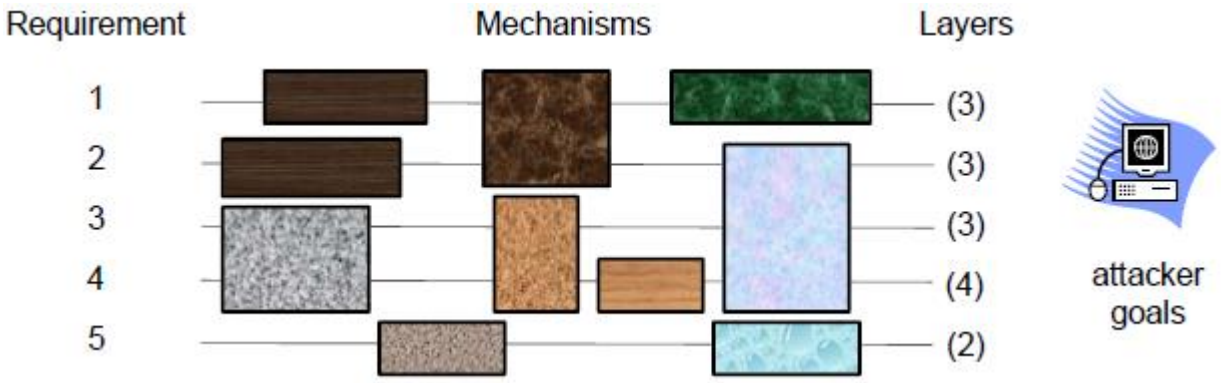
Layered Defense vs. Defense in Depth



Source: http://www.rsaconference.com/writable/presentations/file_upload/star-401.pdf.

Layered defenses, though similar, should not be confused with the defense in depth model. Defense in depth strategies employ several layers of different security functions to protect the system. As a group, the collection of devices protects the system, but each performs a different security function. On the other hand, the strategy of layering commercial devices is predicated on the concept that several layers fulfilling the same security function can ensure that acceptable assurance levels for each security function are met. A security function is a mechanism that transforms, filters, blocks, passes, monitors, or otherwise operates on data or transactions passing between two points in a system in order to support a predefined security policy. The Independent Layer model is different from the defense in depth model in that it requires each component to be sufficient to secure the system should another component be compromised. In other words, each component in each layer of the overall solution is independent of components in the same layer and in adjacent layers of the security hierarchy.

Independent Layer Model



Source: http://www.rsaconference.com/writable/presentations/file_upload/star-401.pdf.

This model limits the likelihood that an attack will succeed by minimizing the points of failure within the overall system. Consequently, an attack on the system is less likely to succeed as the result of the exploitation of an unintentional configuration error or an undiscovered critical vulnerability.

The individual system security requirements are enumerated according to the overall system assurance objectives (confidentiality, availability, and integrity) and its information. The CSfC uses multiple layers of controls, products, and mechanisms to satisfy each requirement. Within each layer, candidate mechanisms are identified, their independence from other mechanisms is assessed, and a collection of mechanisms is selected and composed. The independence and assurance of the solution are assessed and adjustments are made as necessary. The layers are then supplemented with detection mechanisms that monitor the health of the primary mechanisms.

CSfC systems have security through composition. During the design phase, relevant security standards are selected and composed according to the layers of security necessary to address the risk to that system on application. Typically, the number of layers is directly proportional to the level of assurance of the system. Open source and vendor solutions are offered to secure the system according to each separate layer. The solutions can be hardware, software, or hybrid solutions.

Layered security is most effective when different components depend on different algorithms, processors, suppliers, software, protocols, platforms, configurations, operations, and staff. This is known as the layers exhibiting independence. The CSfC model combines security through composition with security through independent layers. The composition of security mechanisms is used to gain assurance that the system will meet the customer security needs. The independence of mechanisms is the primary criterion for assessing members of the composition. By design, the protection mechanisms within each layer are sufficient to protect their own layer, if effective, but not a single point of compromise for the entire system should they fail. Each solution needs only one effective protection mechanism in order to be secure.

The layered assurance of each security requirement can be assessed as a measure of probability. As a result, the layered assurance of the overall solution can be mathematically derived from the level of assurance and independence of the commercial components, as LA = $1- (1-I_1A_1)(1-I_2A_2)…(1-I_nA_n)$, where I_i represents the percent independence of the mechanism, A_i is the percent assurance of the mechanism, and i corresponds to a specific solution out of n total solutions. The assurance of a mechanism depends on the integrity of its processes, its compliance with standards, and its level of testing. It also depends on its record of vulnerability, the reputation and level of trust of its developer, and the trust afforded to the suppliers of its subsystems and components. The independence of a mechanism is dependent on the degree that its factors of independence differ from the factors of all other layered mechanisms. Therefore, if it shares two out of eight factors of independence with other mechanisms (a supplier and administrator for example) then it is 75% independent. Generally, CSfC solutions attempt to maximize the assurance and independence of incorporated components to increase overall security.

Pillar 3: Assurance of Confidentiality and Interoperability

The CSfC initiative assures the confidentiality and interoperability of solutions through the use of Suite B algorithms. Suite B is a category of algorithms that are based on universal commercial standards for application by military, government, industry, and foreign partners. They are designed to be used for encryption, key exchanges, hashing, and digital signatures. Suite B algorithms include Advanced Encryption Standard (AES), Elliptical Curve Diffie-Hellman Key Exchange, Secure Hash Algorithm (SHA), and RSA. The classification level of the information protected and the key strength of the algorithm determine which algorithms are implemented at each classification level (Secret or Top Secret). In some solutions within CSfC, Suite B

algorithms are paired with Internet protocols such as IPSec, Transport Layer Security (TLS), S/MIME, and Secure Shell, to ensure interoperability and confidentiality.

Leveraging the CSfC Program

Agencies with an IA requirement that can be met with a CSfC solution can visit the program website to determine if there is an approved Capability Package to fulfill their needs. If an approved component is available, then the agency can contact the associated vendor for purchasing and implementation information. If a package is not available, then the agency can contact the NSA Client Advocate (CA) to request support. The customer will need to submit an IA requirement for development of a solution by sufficiently documenting the requirement in the Requirements Scoping Questionnaire and by submitting all relevant supporting documentation to the CA. The CA will determine if the CSfC process or another process is best suited to addressing the requirement. If the requirement is a CSfC requirement, then the agency will proceed through the CSfC prototyping phase. An acceptable prototype will be compliant with the Capability Package released in the past two years, unless otherwise noted, and it will present a capability with sufficient deviations from current Capability Packages and previously approved prototypes. Agencies can also request a risk assessment that documents the threats, mitigations, and residual risks associated the CSfC solutions or Capability Packages. Agencies are expected to obtain current versions of the Capability Packages and associated risk documentation and to verify that they have reviewed the current versions. If the agency builds the solution and identifies an issue designing a technologically feasible solution in accordance with the Capability Package requirements, the agency may determine to modify the design to be compliant with the solution. If after the revision or fix to the solution the agency is not able to comply with the Capability Package, the agency should contact the CA.

Vendor Participation

Vendors who wish to have their components eligible as CSfC components in Layered Assurance solutions must submit the component to the NIAP for evaluation and approval in accordance with the applicable U.S. Government Protection Profile(s). The vendor will need to undergo the Federal Information Processing Standards (FIPS) validation process, interoperability testing when it is established, and enter into a Memorandum of Agreement (MOA) with the NSA. According to the NSA, “The MOA obligates the company to provide sufficient information for the NSA to make a risk decision and to cooperate with the NSA to mitigate any discovered vulnerabilities that would impact the risk management posture of the CSfC solution, both initially and throughout the component’s life cycle.” Once a component has

passed the NIAP evaluation, the component will be added to the CSfC Components list and it will be an eligible candidate to serve as a building block in CSfC solutions.

Contact Information

Legislative & Executive Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org


https://twitter.com/ICITorg


https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-


https://www.facebook.com/ICITorg

Sources

Army Communicator:

http://signal.army.mil/armyComArchive/2013/Vol38/No2/NSA%20Implementing%20Commercial%20Strategy.pdf.

National Security Agency:

https://www.nsa.gov/resources/everyone/csfc/
https://www.nsa.gov/resources/everyone/csfc/assets/files/handout-trifold.pdf
https://www.nsa.gov/resources/everyone/csfc/assets/files/csfc-customer-handbook.pdf

RSA:

http://www.rsaconference.com/writable/presentations/file_upload/star-401.pdf.