CEOs of Fortune 500 companies, CIOs of federal/state/local agencies, and average citizens are all concerned about protecting their important information. The National Security Agency protects the nation’s most critical National Security Systems (NSS) and information against cyber-attacks by hardening and defending the cyber infrastructure. Every classified bit of U.S. information traveling across the global infrastructure is protected and encrypted by devices that NSA either certifies, designs, keys or approved for use.

Technological advances have given data owners greater flexibility in accomplishing their business and missions; however, these advances come with a price because every connected device on interconnected global networks now becomes a potential access point for cyber adversaries. The hard truth is despite the fact the U.S. is stronger defensively than it has ever been the number of cyber threats facing the nation have never been greater.

National Security System users require secure access to data anytime/anywhere in order to make timely mission decisions. NSA must be agile and flexible in order to meet the demand signals for rapid deployments of robust cybersecurity encryption solutions. The Agency has a long, proud history of designing/building/testing/fielding/supporting proprietary Government-Off-The-Shelf encryption solutions. It also has a history of strong public-private partnerships with commercial industry. Because of these enduring partnerships, NSA has been able to expand its suite of cybersecurity encryption solutions to include, where appropriate, the use of commercial products and technologies to protect classified National Security System information.

Commercial Solutions for Classified (CSfC) is how NSA is executing its commercial cybersecurity encryption strategy whereby commercial products are architected together in precise ways to protect classified information. CSfC is founded on the principle that properly configured layered solutions can provide sufficient protection of classified data in a variety of different applications.

The oral presentation will highlight CSfC's many activities while also serving as a foundational introduction for those unfamiliar with the initiative. The target audience is everyone interested in learning how they can better protect their sensitive information. Below are the major topics covered during the oral presentation:

**Benefits of Adopting Open Standards and Commercial Products**

There are no releasability issues with commercial equipment, and this makes CSfC attractive in satisfying coalition/diplomatic requirements where the delivered system could be outside the direct control of U.S. personnel. Additionally, commercial devices are not considered Controlled Cryptographic Items (CCI); consequently, there are no special CCI handling caveats or restrictions associated with a CSfC solution. Customers apply existing information technology policies for safeguarding the processing of classified information. Perhaps the greatest benefit realized by national security system customers is the speed with which NSA-approved cybersecurity solutions are delivered. This results in customers being able to leverage commercial products today...while they are still current.

**Designed-In Assurance Features**

Every approved CSfC solution has a number of designed-in assurance features. NSA validates the trustworthiness of CSfC solutions and the components comprising them through a variety of methods:
World-class cadre of NSA systems security engineers design and develop CSfC security architectures; 
Senior NSA technical leaders review the architectures and provide oversight on all CSfC capabilities; 
Customer registrations of CSfC solutions provide NSA’s cybersecurity leadership with the requisite situational awareness regarding which components are being used and where; 
Commercial components are tested against published U.S. Government and collaborative Protection Profiles and internationally recognized Common Criteria security requirements; and 
Customer-led certification and accreditation testing ensures compliance with NSA standards for the protection of classified information.

**Capability Packages**

Capability Packages (CP) are the system-level foundation for this strategy. They provide use-case descriptions of the operational capabilities, along with the accompanying security architectures. These solution designs have vendor-agnostic information that enables customers and integrators to implement their own solutions. Using the information in these Capability Packages, customers/integrators make product selections from the CSfC Components List while following the specifications to create an architecture with specific commercial products configured in a particular manner.

**Protection Profiles**

U.S. government Protection Profiles serve as the product-level foundation. They contain the technology-specific security requirements needed in various components. Protection Profiles are the mechanisms by which the U.S. Government conveys to commercial manufacturers the security features needed to protect classified information. Once a vendor builds a commercial component that meets the requirements of one or more Protection Profiles, that vendor submits the component to one of the authorized Common Criteria labs for compliance testing. This commercial lab testing is accomplished more quickly and inexpensively than in the past due to significant transformations to generate Protection Profiles written in precise, testable language.

**Managing Risk**

Deciding what constitutes acceptable risk is always an important consideration for data owners. Raising the bar in a security solution to mitigate vulnerabilities often comes at the expense of both development resources and operational efficiencies. Calculated risk-management decisions must occur with leadership’s eyes wide open. Commercial cybersecurity products must deliver a quality user experience that meets the requisite security policies without sacrificing operations.

NSA’s Deputy National Manager for National Security Systems is responsible for deciding what is sufficient for protecting classified U.S. information. The Capability Packages represent approved techniques involving commercial products that are suitable for protecting classified information. CSfC is here now – it is in practice today. Over 10,000 users across dozens of sites including civil and military agencies are using or preparing to use composed commercial cybersecurity solutions.
**Trusted System Integrators**

Trusted system integrators are instrumental to CSfC’s success because they serve as the honest brokers for decision makers who will be responsible for approving the use of commercial cybersecurity solutions at their sites. To ensure there is a cadre of qualified trusted integrators, NSA has vetted/approved 70+ commercial system integrators, many with a global presence, who can assemble/integrate commercial cybersecurity products according to NSA requirements.

**CSfC’s Bright Future**

Although NSA’s strategy for protecting classified information continues to employ both commercially based and traditional GOTS cybersecurity encryption solutions, National Security System customers increasingly are looking first to commercial technology and solutions to satisfy their operational needs. These government customers like CSfC because it allows them to get commercial cybersecurity solutions deployed faster. Policymakers also like CSfC because of NSA’s reputation of protecting information and for outmaneuvering adversaries. And last but certainly not least, industry likes NSA’s commercial model because it fully leverages the energy and innovation of the private sector.