VOLUME 1
ISSUE 2
November 2018

CSfC Bits & Bytes

A Quarterly Newsletter Highlighting CSfC

In this issue:

CSfC Tech Talks

have proven to be very successful. In that light, we have decided to make them a regular monthly event.

Miss the one on November 8th? We hope to have one more before the December holidays - Stay tuned for more info…

Topics vary, and the discussion is shaped by you – our customers.

Attendance is limited to the first 75, so bring your questions and signup early!

Send signup request to:
csfc@nsa.gov
Subject: CSfC Tech Talk

Want to subscribe to this Newsletter?

Send email to: csfc@nsa.gov
Subject: Newsletter Subscription

From the Director's Desk…

Exciting changes are in the air –

Welcome to the 2nd issue of the CSfC Newsletter

Our inaugural issue was very well received -- we had many requests from you to be added as recipients. Thank you for all the feedback and positive comments. We use your input to scope the content, so please keep it up…

As always, reach us at csfc@nsa.gov

Meet the new CSfC Director!

Congratulations to Mr. John Dunker
Director, Commercial Solutions for Classified (CSfC)

Last month, the Commercial Solutions for Classified Program Management Office said goodbye to its CSfC Director, Crisantito Valencia. Chris was instrumental in shaping the direction of the CSfC program and we wish him well as he is promoted on to exciting new opportunities within the Agency.

We are fortunate this month to be able to welcome the new Commercial Solutions for Classified Director, Mr. Thomas "John" Dunker. John is a career NSA employee with many years of experience in IT and Information Assurance. He is well known and respected throughout our community and brings a wealth of knowledge to the Commercial Solutions for Classified (CSfC) Program. Prior to his appointment as the CSfC Director, John served on a Joint Duty Assignment to the Pentagon, gaining a keen appreciation of the needs of our DoD customers.

Please join us in welcoming him to the CSfC team!

What's Happening in CSfC

CSfC Takeaways

Customers

Engage CSfC early when implementing solutions – tailored exceptions discovered late in the process could significantly delay the approval

Component Vendors

Develop products that meet US/Collaborative Protection Profile requirements – see NIAP/Common Criteria evaluations

Authorizing Officials

Confirm compliance with the Capability Packages and ensure solutions are registered with the CSfC PMO

Trusted Integrators

Engage CSfC with innovations beyond the CP specifications

Acquisition/Procurement

Require that products from the CSfC Approved Components List are a mandatory part of your procurement activities

Recently Added Trusted Integrators

- NAVAIR Naval Air Warfare Center–Aircraft Division
- NexTech Solutions LLC
- Cambridge International
- CyberIP Services
- Peraton
- Rockwell Collins

Notable on the CSfC Website:

- Improvements to the Solution Registration documents, particularly the Compliance Checklists. These changes are aimed to clarify and streamline the Solution Registration process across all CPs
- CSfC Threat Prevention Slicksheet
- Archived Trusted Integrator Page
- Enterprise Gray Implementation Requirements Annex

Stakeholder Engagement Highlights

Recently

- 13-17 AUG (Omaha, NE): DoDIIS Worldwide Conference *(Keynote Speaker)*
- 17-21 SEP (Rome, IT): Multinational Maritime Information Interoperability (M2I2)
- 02 OCT (Baltimore, MD): CSfC Tech Day *Sponsored by Mercury Systems*
- 09-10 OCT (Baltimore, MD): Cyber Maryland Conference

Upcoming

- 05-08 NOV (San Antonio, TX): Alamo AFCEA ACE
- 12-16 NOV (Augusta, GA): AFCEA TechNet (Keynote Speaker)
- 03-06 DEC (Centcom): Site Visit
- 27 JAN-02 FEB (Canberra, Aus) Multinational Maritime Information Interoperability (M2I2)

CSfC Approved Components

- Getting a component on the CSfC "approved" list is an investment in both time and money, however it could be a sound investment as many Government procurements require this approval
- All components must be US or Common Criteria validated
- CSfC Selections are additional criteria, beyond the NIAP specifications, needed to be CSfC approved
- A component may be "archived" because a vendor chooses not to pursue the NIAP Assurance Continuity process or because the component has been superseded by new NIAP-approved versions. An archived component can continue to be used in an existing operational CSfC solution for a period of time, however new registrations must use a current CSfC component

Recently Approved Components

IPsec VPN Client:

- Samsung Galaxy Note 8, Android 7.0 and 8.0
  (NIAP validation complete)
- Samsung Galaxy S8, Android 7.0 and 8.0
  (NIAP validation complete)

IPsec VPN Gateway:

- Cisco Firepower Threat Defense on ASA and Virtual Firepower Threat Defense
  (NIAP validation ongoing)
- Cisco Cloud Service Router 1000v and Aggregation Services Router (ASR) 1000 series
  (NIAP validation complete)
- PacStar 351, 451, 455 and 551 with Cisco ASAv, v9.6
  (NIAP validation ongoing)
- Cisco NGFW running ASA v9.8 and FX-OS v2.2 on Firepower 2100 series, v6.1
  (NIAP validation complete)
- Architecture Technology Corp. Compact rugged Router CRR-1000, v1.0
  (NIAP validation ongoing)
- Cisco Firepower Threat Defense v6.2 and FX-OS v2.2 on 4k & 9k Families
  (NIAP validation ongoing)
- Cisco Firepower Threat Defense v6.2 and FX-OS v2.2 on 2k Families
  (NIAP validation ongoing)
- Aruba 600 Series Mobility Controllers OS 6.5-FIPS
  (NIAP validation complete)
- Aruba 3000 Series Mobility Controllers OS 6.5-FIPS
  (NIAP validation complete)
- Aruba 6000 Series Mobility Controllers OS 6.5-FIPS
  (NIAP validation complete)
- Aruba 7000 Series Mobility Controllers OS 6.5-FIPS
  (NIAP validation complete)
- Cisco ESR 5900 series
  (NIAP validation complete)
- Palo Alto Networks, Next Gen Firewall, PAN-OS 8.0.6
  (NIAP validation complete)
- Palo Alto Networks, Net Gen Firewall, specified configurations, PAN-OS 8.0.6
  (NIAP validation complete)

MACSEC:

- Cisco ASR 9000 product series, v6.1
  (NIAP validation complete)
- Cisco Catalyst 3650 and 3850 series switches, IOS-XE 16.3
  (NIAP validation complete)
- Cisco Catalyst 9300 and 9500 series switches, IOS-XE 16.6
  (NIAP validation complete)

Software Full Disk Encryption:

- Curtiss-Wright Defense Solutions, Compact Network Storage 4-Slot Software Encryption Layer, CentOS (Linux)
  (NIAP validation ongoing)

Component Categories

- CSfC component categories follow those used by NIAP
- Register under multiple categories if possible and reasonable

Pointers for a smoother Solution Registration

- The number of registrations has increased, causing the approval time to increase correspondingly. The PMO is working on reducing the time from, however current solution registration time – from submission to signature - has increased from a 3-4 month average to a 3-6 month average
- Smooth your Solution Registration Process:
  - ✓ Ask questions early
  - ✓ Include Overview 1 (OV-1) diagrams with selectable components and model numbers clearly labeled

Questions?
Email the CSfC team at:
csfc_register@nsa.gov

Recently Approved Components - *Continued*

IPS:
- Cisco Firepower Threat Defense on ASA and Virtual Firepower Threat Defense (specified series) v6.2; (NIAP validation ongoing)
- Cisco Firepower Threat Defense v6.2 and FX-OS v2.2 on 4k & 9k Families (NIAP validation ongoing)
- Cisco Firepower Threat Defense v6.2 and FX-OS v2.2 on 2k Families; (NIAP validation ongoing)
- Cisco Firepower (specified series) v6.1 (NIAP validation complete)

Specific product details always available on the CSfC website at:
https://www.nsa.gov/Resources/Everyone/csfc/Components-List/

TLS Software Application:
- Enveil, ZeroReveal Compute Fabric, V1.1.1 (NIAP validation complete)
- Nubo Software Thin Client, v2.0 (NIAP validation complete)

Traffic Filtering Firewall:
- Cisco Firepower Threat Defense on ASA and Virtual Firepower Threat Defense (NIAP validation ongoing)
- F5 Networks BIG-IP, BIG-IP TMOS (Common Criteria validation ongoing)
- PacStar 351, 451, 455 and 551 with Cisco ASAv, v9.6 (NIAP validation ongoing)
- Cisco Firepower Threat Defense v6.2 and FX-OS v2.2 on 4k & 9k Families (NIAP validation ongoing)
- Cisco Firepower Threat Defense v6.2 and FX-OS v2.2 on 2k Families (NIAP validation ongoing)
- Cisco NGFW running ASA v9.8 and FX-OS v2.2 on Firepower 2100 series, v6.1 (NIAP validation complete)
- Palo Alto Networks, Next Gen Firewall, PAN-OS 8.0.6 (NIAP validation complete)
- Palo Alto Networks, Net Gen Firewall, specified configurations, PAN-OS 8.0.6 (NIAP validation complete)
- Forcepoint Federal Next Gen Firewall, Linux v6.3.1; (NIAP validation complete)
- Aruba 600 Series Mobility Controllers OS 6.5-FIPS; (NIAP validation complete)
- Aruba 3000 Series Mobility Controllers OS 6.5-FIPS; (NIAP validation complete)
- Aruba 6000 Series Mobility Controllers OS 6.5-FIPS; (NIAP validation complete)
- Aruba 7000 Series Mobility Controllers OS 6.5-FIPS; (NIAP validation complete)

Authentication Server:
- Cisco Identity Services Engine v2.2; (NIAP validation complete)

SIP Server:
- Cisco CUCM v11.5; (NIAP validation ongoing)

Mobile Platform:
- Samsung Research America, Galaxy Tab S4, Android 8.0 & 8.1 (NIAP validation complete)
- Samsung Research America, Galaxy Note 9, Android 8.0 & 8.1 (NIAP validation ongoing)
- Samsung Galaxy Note 8, Android 7.0 and 8.0 (NIAP validation complete)
- Samsung Galaxy S8, Android 7.0 and 8.0 (NIAP validation complete)

An Introduction to Protection Profiles

A **Protection Profile (PP)** is an implementation-independent specification of information assurance security requirements. PPs contain technology specific threats, security objectives, security related functional requirements, and evaluation activities. PPs are developed in Technical Communities (TCs) comprised of Government, industry, and academia experts with the goal of obtaining achievable, repeatable, and testable evaluation activities for each technology.

A **collaborative Protection Profile (cPP)** is similar to a Protection Profile, but created through an international Technical Community (iTC) with a sponsorship from 2 or more Common Criteria Recognition Arrangement (CCRA) nations.

A **PP-Module (MOD)** or **Extended Package (EP)** further refine security requirements from those included in a base PP or cPP. A base PP/cPP contains security requirements for a given technology type. The MOD/EP adds to the requirements of a PP/cPP to address a subset of that technology. For example, the Network Device cPP (NDcPP) contains security requirements that any network device must meet, and the WIDS/WIPS EP extends from the NDcPP to add requirements that are specific to a WIDS/WIPS. A vendor that wishes to evaluate their product against a MOD or EP must meet all the mandatory requirements of the MOD/EP and its base PP/cPP.

A product is issued a **NIAP certificate** upon successful completion of NIAP evaluation. Testing of the product against a Protection Profile is done by a NIAP-approved Common Criteria Testing Lab (CCTL) which is accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).

CSfC selections define the specific PP requirements that must be included as part of a Common Criteria Evaluation for a product to be eligible for use in a CSfC solution.

Protection Profiles in Development

NIAP is currently working with industry, customers, and the Common Criteria community to create Protection Profiles (PPs) for each technology. These PPs include assurance activities with the goal of achievable, repeatable and testable evaluation activities for each particular technology.

NIAP is in the process of updating its list of PPs in Development --- Stay tuned for an update in the next issue of this newsletter.

*For additional information, please send inquiries to niap@niap-ccevs.org

More Information at:

https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm

CSfC Points of Contact:

General Inquires:
csfc@nsa.gov

Client Contact Center:
IAD_CCC@nsa.gov

CP Specific Inquires:

MA CP:
Mobile_Access@nsa.gov

MSC CP:
MSC_CP@nsa.gov

WLAN CP:
Wi-FI@nsa.gov

DAR CP:
CSfC_DAR_Team@nsa.gov

Next CSfC Tech Talk:

- 8 Nov 2018
- 1500 -1600
- Register by emailing:

  csfc@nsa.gov

  with Subject:

  CSfC Tech Talk

What is Coalition Gray?

- Coalition Gray is simply another step in the Enterprise Gray evolution, designed to support our coalition allies.
- Coalition Gray is still in the "concept" phase, with a scoping meeting targeted for the Jan 2019 timeframe.

CSfC Tech Talks

CSfC "Tech Talks" are a monthly, one hour, dial-in with CSfC technical professionals. The talks are open to customers, vendors and trusted integrators. The topics are dictated by the participants – you ask the questions.

The first CSfC tech talk was held on 27 September 2018 and chaired by the CSfC Technical Director. Several consistent themes arose during the discussion, resulting in several requests for additional, focused discussions, to include:

- Streamlining the Solution Registration Process
- Implementing a "multi-year" solution registration to ease renewals
- Purpose and direction of Enterprise Gray
- Potential of increasing the Approved Component "lifespan"
- Difficulty in registering an End User Device without owning the operating system(s)

Updates and discussion on these topics will be addressed at the upcoming November Tech Talk. We hope to fit in another Tech Talk in December.

Enterprise Gray Implementation Requirements Annex

The Enterprise Gray Implementation Requirements Annex is designed to address the increasing demands by customers who desire to implement CSfC solutions across geographically wider distances while leveraging existing infrastructure and services to manage them.

This Annex provides cost effective techniques to deploy the three data-in-transit Capability Packages -- Campus Wireless Area Network, Mobile Access, & Multi-Site Connectivity-- at the same time, using centralized certificate and VPN management.

The initial comment period for this Annex has closed, thanks to all who contributed. The comments will be adjudicated and incorporated as the Enterprise Gray CP Annex marches nearer to completion. Estimated target timelines are:

- Week of 10 Dec 2018 Obtain Technical Advisory Council concurrence
- Week of 31 Dec 2018 Obtain National Manager Approval & Publish v1.0

CSfC Threat Prevention

- The CSfC Program develops Capability Packages in order to provide customers with ready access to the information needed to use COTS in their daily operations and protect their data against today's threats that aim to exploit NSS networks
- Learn more with the recently published Threat Prevention slicksheet at:

https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/threat-prevention.pdf

CP Updates and Roadmaps

CSfC Capability Packages provide high-level reference designs and corresponding configuration requirements, allowing customers to select COTS products from the CSfC Components List and properly configure those products to achieve a level of assurance sufficient for protecting classified data. CPs are not static documents; they are constantly evolving to meet customer needs and incorporate technology advances. As does any useful product, CPs operate on a lifecycle – from concept need to initial publication, followed by multiple release updates, as applicable, to continue to best support customer needs.

The CP Development Lifecycle Phases:

1. ***Requirements Gathering***: Requirements are derived from multiple sources – registration deviations; use cases; RFIs; new products; vulnerabilities; NIAP PPs – to name a few. If you have a need beyond what a CP specifies, engage the CSfC PMO
2. ***Internal/External Comments***: Requirements are assessed, vetted and assembled into a draft release. The draft is validated through pre-publication review and posted to the CSfC website as a "point 8" draft. Community comments to this draft are collected for a specified period. Comments are adjudicated, and feedback is provided
3. ***CP Release***: After the comment cycle is complete, the initial CP (or the next major release of an existing CP) is finalized. This is a detailed process that includes the development of a Testing Annex and a Compliance Matrix. The final Risk Assessment is also completed in this phase. All documents are assembled and presented to a Senior Technical Advisory Committee (TAC) for review and approval. This could take several iterations, but once approved, the package is forwarded to the Deputy National Manager for signature.

A Capability Package's status can be identified as follows:

- 0.8 a draft version, posted to the website for comment
- 1.0 an initial released version of a CP
- x.1 a minor update to an existing CP; repeated as necessary (e.g. x.2)
- 1.8 a draft CP released for comment only
- 2.0 a major update to an existing CP; repeated as necessary (e.g. 3.0)
- annex a self-contained portion of a CP that can be applied to multiple CPs

CP updates on the horizon include:

- Key Management and Enterprise Gray Annex updates
- Next-Gen (EUD and Infrastructure)
- Continuous Monitoring CP