VOLUME 1
ISSUE 1

July 2018

CSfC Bits & Bytes

A Quarterly Newsletter Highlighting CSfC

In this issue:

Notable bits:

- Every bit of US classified information traveling around the global enterprise is protected by technology designed, certified, keyed or approved by NSA
- CSfC is how NSA executes its commercial cybersecurity strategy – architecting commercial products together in precise ways to protect classified information

Want to subscribe to this Newsletter?

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

From the Director's Desk…

The CSfC Team

Welcome to ***CSfC Bits & Bytes***, a quarterly newsletter designed to provide updates, direction and information about the Commercial Solutions for Classified program. In each issue, we aim to provide short "bytes" of information useful to our customers, integrators and component vendors.

This inaugural issue is a direct result of feedback received from you. We are committed to providing improved dialog and more timely information about the program, its ongoing technical direction, capability updates, program processes, technical improvements, and other information of interest to you.

We hope you find this newsletter to be useful – comments and suggestions always welcome.

Reach us at: csfc@nsa.gov

Give us your thoughts on the CSfC Program Office hosting a monthly

– ***CSfC Tech Talk***–

an hour-long, dial-in, round table discussion with the CSfC Technical Director and Engineers, open to Customers, Integrators & Vendors.

Interested? Send comments to: csfc@nsa.gov

Subject: CSfC Tech Talk

What is the "NextGen" Project?

- The Cybersecurity Solutions group is developing & testing a Next Generation reference implementation for wireless connectivity to evolve into a future CSfC Mobile Access Capability Package
- This current proof-of-concept was designed as a reference implementation and is not intended to specify the use of specific brands of equipment

CSfC Program Growth

- CSfC has experienced a 200% increase in customer solution registration requests over the past year
- Customer requests for renewals of operational solutions has reached the 90% mark

Recently Approved Trusted Integrators

- Augustine Consulting, Inc.
- CSRA LLC
- Futron, Inc.
- The MIL Corporation
- Verizon

Recently Approved Components

File Encryption:

Trivalent Protect for Android running v2.6

Mobile Platform:
Samsung Galaxy Devices running Android 8.0
Apple iOS11 iPhone/iPad Devices running iOS v11.2

IPsec VPN Client:

Cisco AnyConnect Secure Mobility Client for iOS v4.6
Samsung Galaxy Devices running Android 8.0

IPsec VPN Gateway:
Juniper SRX Product Series running JUNOS 17.4
Cisco ISR 1100 Product Series running iOS-XE 16.6
Cisco NGFW running FP v6.1
Cisco ASA 5500 Series running v9.6/v9.8
Cisco ASAv running v9.6/v9.8

More details are always available on the web:

https://www.nsa.gov/resources/everyone/

Software Full Disk Encryption:
Curtiss-Wright DTS1 Software Encryption Layer v1.0

Mobile Device Management:
Apple iOS11 iPhone/iPad Devices running iOS v11.2

IPS:
Juniper SRX Product Series running JUNOS 12.3/17.4

TLS Software Application:
Intelligent Waves Hypori Client running v4.1

Traffic Filtering Firewall:
Juniper SRX Product Series running JUNOS 17.4
Cisco NGFW running FP v6.1
Cisco ASAv running v9.6/v9.8
Cisco ASA 5500 Series running v9.6

Good Cyber Hygiene

- Ensure your CSfC components are properly configured and patched
- Remember that consistent application of authorized vendor patches is critical to maintaining good cybersecurity hygiene!

More Information at:

https://www.niap-ccevs.org/Profile/InDraft.cfm

Recently Archived Components

IPsec VPN Client:

Cisco 5921 ESR running iOS 15.5
Cisco AnyConnect Desktop 4.1

Traffic Filtering Firewall:

Cisco ASA 5500-X Series Appliances running v9.4
Cisco ASAv running v9

Mobile Device Management:

MobileIron Mobile Device Management Solution

IPsec VPN Gateway:

Brocade MLXe Family Devices running IronWare
Cisco 5915/5940 ESR running iOS 15.5
Cisco ASA 5500-x Midrange Appliances v9.4
Cisco ASAv running v9.4

Components are normally archived either because the manufacturer chooses not to pursue NIAP's Assurance Continuity Process or because the component has been superseded by new NIAP-approved versions

Protection Profiles (PPs)

NSA works with technical communities from across industry, government, and academia to develop and publish product-level requirements in US Government Protection Profiles (PPs). Protection Profiles are an implementation-independent set of security requirements and test activities for a particular technology, enabling achievable, repeatable, and testable evaluations. These PPs define security measures and assurance requirements that clients, integrators, and commercial component developers expect components to meet. Commercial component developers can apply these requirements and make judgements about the security attributes of their products. All products evaluated must demonstrate exact compliance to the applicable technology protection profile.

Looking Ahead

Protection Profiles in Development	Estimated Completion
Peripheral Sharing Device v4.0	CY2018 Q2
SSL/TLS Inspection Proxy v1.0	CY2018 Q3
Software File Encryption v2.0	CY2018 Q4

Areas also under consideration:

- Updated WIDS/WIPS EP
- IPMS PP

What features might be included in future Capability Package Releases?

- WPA3
- Crypto Diversity between CAs
- Local and Remote crypto erase
- Data Reconstitution

An Important "tidBIT" of Information for all CSfC Customers…

- Please ensure all submitted registration packages contain solution diagrams. We want your solution to be registered as quickly as possible
- Questions? Email the CSfC team at:

  csfc_register@nsa.gov

What's New with Capability Packages (CPs)?

In order to improve consistency across all Capability Packages and to allow for more efficient updates and revisions, existing CPs are being reorganized into a more modular configuration – resulting in a "base" CP and associated "annexes" that could apply to more than one base CP.

The first of these new annexes scheduled for release is the *Key Management Requirements Annex*. Once published, the data-in-transit CPs (Mobile Access, Campus Wireless LAN and Multi-Site Connectivity) will point to this common Key Management Annex to ensure consistent application of requirements.

Capability Package annexes in the works include:

- Key Management Annex
- Enterprise Gray Annex
- Continuous Monitoring Annex

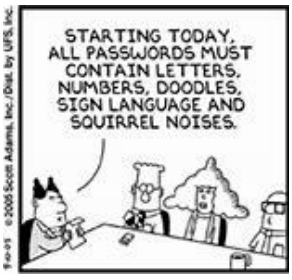
What is Enterprise Gray?

NSA's Cybersecurity Solutions is delivering the Enterprise Gray (EG) Implementation Requirements Annex to meet the increasing demands by customers who desire to implement CSfC solutions with the following characteristics:

- Ability to implement multiple capability packages simultaneously
- Capable of centralized management
- Readily scalable
- Enhanced site-survivability

Random Password Generator (RPG) available

- Available for use as a password/phrase generator – currently only for application with DAR CP v4.0
- Projected to be officially released for both RPG and Random Key Generator (RKG) applications after some additional testing
- Current version available by email, contact CSfC@nsa.gov



We Want to Hear from You…

- In future issues we want to highlight your experiences with CSfC
- Submit your short, unclassified article to csfc@nsa.gov with Subject: News Article
- Please keep the length of each submission to no more than 1000 words
- Send along any unclassified photos too. This is a great way to spread the word!

On the Road and Around the Globe

- CSfC was at **The Atlantic Security Conference** in **Halifax, Nova Scotia, Canada**. This non-profit security conference involved many minds coming together with the goal to expand the pool of IT Security knowledge. CSfC's Communication Manager spoke on a wide variety of CSfC activities with a particular emphasis on the growing public/private partnerships and the role CSfC plays in NSA's overall encryption solutions strategy to ensure the right cybersecurity solutions are available to stakeholders.

- CSfC participated at the **Cybersecurity Leadership Forum** at the Newseum in **Washington, DC**. This conference brought together leaders from across government and industry to share how our nation's citizens and critical assets are protected against cyber adversaries. CSfC highlighted the Encryption Solutions products and how that translates to the leveraging of commercial technologies when appropriate.

- CSfC traveled across the pond to **Camp Arifjan, Kuwait** as part of the **Best Cyber Ranger 2018** competition to promote cybersecurity awareness. CSfC's Communication Manager delivered one of the keynotes and served as a competition judge.

Stakeholder Engagement Highlights

Recent Industry/Customer Engagements

- 07-11 May (Camp Arifjan, KU): Best Cyber Ranger 2018
  Sponsored/hosted by ARCENT/335th Command
- 16-17 May (Baltimore, MD): AFCEA Defensive Cyber Ops Symposium
- 11-15 June (Orlando, FL): Cisco LIVE
- 12-13 June (Wash, DC): 2018 Cybersecurity Leadership Forum
  Sponsored by Forcepoint

Recent and Upcoming Events

- 17-19 July (Hagerstown, MD): Connecting Next-Generation Solutions Technical Summit
  Sponsored by B&D Consulting
- 13-15 August (Omaha, NE): DODIIS Worldwide Conference
- 17-21 Sept (Rome, IT): Multinational Maritime Information Interoperability (M2I2)
- 2 Oct (Baltimore, MD): CSfC Tech Day
  Sponsored by Mercury Systems

Questions from the website

- The CSfC website -

  csfc@nsa.gov

  receives hundreds of questions from current and potential vendors, integrators, and customers from around the globe
- The mailbox is monitored every business day
- Adjacent are some frequently asked questions and corresponding answers

CSfC Q&A

1. What are the downsides of NOT using a CSfC integrator? Could we just as easily submit the package without one?

There is no requirement for a customer standing up a CSfC solution to utilize an Integrator from our list, so yes, if your organization feels that they have the expertise, they can act as their own integrator and submit the registration package on behalf of their customer.

Some of the benefits of using an integrator from our list are:

- they have been vetted by NSA through an application and interview process
- they may have prior experience in integrating other similar solutions
- they may have experience in selecting and configuring the right components in the right way
- they have an understanding of how to navigate the registration process and associated documentation needed

Unfortunately, CSfC is not able not make recommendations on selecting an integrator and does not track or list them by specialty.

2. What is the process to become a Trusted Integrator (TI)?

The process to become an Integrator is pretty simple. A company fills out and submits the application. Once received, it is reviewed, and a face-to-face meeting is scheduled here at the Agency.

After the meeting, a yes/no determination is made by the CSfC office. If approved, a Memorandum of Agreement (MOA) is drafted, signed by the CSfC Director, then sent to the company for review. This process takes roughly 30-45 days. There is no cost to the vendor other than any internal costs to fill out the application, attend the meeting and review the MOA.

3. How do I get a CSfC registration number and what's next?

Initiate the process by sending an email to the CSfC team at csfc_register@nsa.gov to receive a Registration ID number; it will look something like: CSfC-X-ORG-CP-2018-0099.

The next step is to submit your registration package for review. If there are any questions or discrepancies that arise during the review, we can work with your organization to get them resolved. To get started, you will need to submit:

- Registration Form (it does not require an AO signature at submission)
- Compliance Checklist
- Network Diagram/Solution Architecture
- Deviation Request Form (for each requirement you are unable to meet)
- Concept of Operations Document

The Registration Form and Compliance Checklist are available online at: https://www.nsa.gov/resources/everyone/csfc/solution-registration.shtml

You will need to create the Network Diagram; high-level examples can be found in each Capability Package. Please include product make/model in the diagram – this will make it easier for the review team to identify components.

The Concept of Operation Document is a 'one-pager' explaining the "*who, what, why, where, when & how*" of your solution. This high-level description allows us to better understand what the CSfC solution will accomplish and make corresponding assessments.