How to Operate Remotely On Multiple Network Classifications Using Cross Domain And CSfC

Tony West
Forcepoint Global Governments & Critical Infrastructure

Dylan Connor
ID Technologies
Meet Today’s Speakers

Tony West
Global Governments & Critical Infrastructure, Forcepoint

Dylan Conner
Chief Technology Officer, ID Technologies
Today’s Agenda

Requirement: Multi-Domain Operations to Enable Remote Workforces

CSfC and Cross Domain – Government Programs Designed to Enable

- Commercial Solutions for Classified
- Cross Domain Solutions (Transfer and/or Access)

Architecture

- Cross Domain Solution (access/transfer levels 2x), End User Device, Mobility Access Capability Package “MCAP”
- Forcepoint enabling automation // managing gray (extension of current function)

Practical Considerations for CSfC and Cross Domain

- Repeatable/trusted enablement cost, way you can run it
- Implementation / accreditation / O&M
Requirement: Enable Remote User with an Experience Similar To Office

01. Enable Remote Workforces
   • Increase capabilities of existing remote users.
   • Provide remote work capability to workforce that traditionally worked in the office.

02. Provide Access to Unclass and Class Networks and/or OGA’s
   • Enable secure access to required networks: Low and High
   • Home office or in the field

03. Manage Cost and maintain security
   • Ensure positive experience to end user – avoid the “bad.”
   • Automate Processes
   • Decrease cost, complexity, and management overhead of currently available solutions
CSfC & Cross Domain

NSA/CSS's **Commercial Solutions for Classified (CSfC)** Program has been established to enable commercial products to be used in layered solutions protecting classified NSS data.

**Capability packages** include multi-site connectivity communications, data at rest solutions, campus wireless local area networks and mobile access solutions.

**Cross Domain – Controlled, ITAR technology. Governed by NSA: NCDSMO**

- Transfer – movement of data between enclave classifications, in-agency or cross-agency (ex: HSG)
- Access – presentation of multiple enclave user environment via Cross Domain “Distribution Console.”
The CSfC Program’s Key Players

**The National Security Agency/Central Security Service (NSA/CSS)**
- Oversees program
- Reviews, certifies CSfC solutions

**Component Suppliers**
- Approved vendors of applicable products built in accordance with the applicable USG profiles and Common Criteria Processors

**Trusted Integrators**
- Approved to architect, design, integrate, test and support CSfC solutions

**Customers**
- Dept of Defense
- Intelligence Community
- Federal Civilian
Notational HSG Log Aggregation Architecture
There are lots of perspectives on the best way to “do” CSFC.

CSFC pro-tips:

1. Use a design that you know works.

2. Use a design that you know your organization can sustain.

3. Documentation is more important that the last “nth” percent.

4. Cross domain transfer (Forcepoint High Speed Guard) is your friend:
   - Cross Domain security log shipping
   - Cross Domain certificate management
   - Cross Domain event correlation and troubleshooting

5. The best way to do CSFC is the way that gets deployed and used.
ID Technologies offers a complete turn-key CSfC mobility solution. Combined with Forcepoint’s Cross Domain solutioning, and our purpose built “Zero Vulnerability” client, Agencies are able to rapidly pivot towards managed, secure remote user access. [https://www.idtec.com/archon-zv/](https://www.idtec.com/archon-zv/)
Thank you

Get in Touch:

Tony.West@forcepointgov.com
Dylan@idtec.com