Committee on National Security Systems

CNSS Advisory Memorandum
Information Assurance 01-15
April 2015

ADVISORY MEMORANDUM

USE OF COMMERCIAL SOLUTIONS TO PROTECT NATIONAL SECURITY SYSTEMS

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems (CNSS) is issuing this Advisory Memorandum (AM) to inform agencies how to safeguard National Security Systems (NSS) when using a Commercial Solutions for Classified (CSfC) solution. A CSfC solution, when properly implemented according to requirements and standards established and approved by the National Security Agency (NSA), may be used to protect NSS and the information therein.

2. This Advisory Memorandum provides guidance to U.S. Government (USG) Departments and Agencies (D/As) as to the responsibilities for maintaining the security posture of NSS using CSfC solutions, and provides guidance on the minimum set of security measures required for the use of CSfC solutions in a national security environment. For this advisory, the term D/A shall be interpreted to include Federal bureaus and offices. The heads of D/As are ultimately responsible for protecting NSS (both unclassified and classified) that transmit, receive, process, or store information using CSfC solutions. D/As must ensure that all CSfC solutions comply with NSA requirements, as delineated in this advisory.

3. This advisory incorporates and supersedes CNSSAM 01-12, *NSA-Approved Commercial Solution Guidance*, dated June 2012. This advisory is being issued in accordance with CNSS Directive (CNSSD) No. 901, *Committee on National Security Systems (CNSS) Issuance System*, dated September 2012 (Reference a).

4. For further information, please contact the NSA Information Assurance Directorate's Office of Client Engagement at (410) 854-4790.

5. This advisory is available from the CNSS Secretariat, as noted below, or the CNSS website: www.cnss.gov.

FOR THE NATIONAL MANAGER:

/s/

CURTIS W. DUKES

ADVISORY MEMORANDUM
USE OF COMMERCIAL SOLUTIONS TO PROTECT NATIONAL SECURITY SYSTEMS

SECTION I – PURPOSE

1. CSfC solutions, when implemented according to NSA requirements, are capable of protecting classified and sensitive information. This advisory memorandum outlines those requirements for securely implementing CSfC solutions to protect NSS.

SECTION II – AUTHORITY

2. The authority to issue this advisory memorandum derives from National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (Reference b), which outlines the roles and responsibilities for securing NSS, consistent with applicable law, Executive Order 12333 (Reference c), as amended, and other Presidential directives.

3. Nothing in this advisory should be interpreted as altering or superseding the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This advisory memorandum applies to all USG D/As and appropriately cleared USG contractors that use or plan to use, implement, or test CSfC solutions to protect NSS. It also applies to the processes that enable the D/A to oversee the planning, design, development, acquisition, deployment, implementation, upgrade, use, control, operation, maintenance, and disposition of existing and future CSfC solutions within their scope of authority.

SECTION IV – BACKGROUND

5. The USG protects NSS through the use of both CSfC solutions and NSA-certified Information Assurance (IA) products. Using NSA-approved CSfC solutions allows D/As to keep pace with technological progress and employ the latest capabilities in their systems and networks. D/As are able to reduce the time it takes to build, evaluate, and deploy IA solutions by utilizing mature technologies already available in the commercial sector.

6. CSfC solutions employ a layered approach to meet the security requirements necessary to adequately protect NSS. Capability Packages (CPs) outline a minimum set of

standards for CSfC solutions, and provide the IA community with a sufficient level of assurance. CPs are approved by the National Manager.

7. CSfC solutions differ from NSA-certified IA products in significant ways. The security boundary is different, as CSfC requires two independent layers of encryption creating a space between the red and black networks known as the “gray network.” CSfC solutions also require that D/As assume a more significant role in understanding, managing and determining whether to accept the risks associated with the implementation of a solution. Finally, CSfC solutions require D/As to configure a layered solution using approved commercial components according to a CP, rather than deploying a single certified product.

SECTION V – GUIDANCE

8. A CSfC solution, whose operational use has been approved by the appropriate Authorizing Official (AO) as being compliant with an NSA-provided CP, may be used to protect NSS and the information therein.

9. The NSA provides CPs specifying the requirements for the implementation of CSfC solutions. Each D/A using CSfC solutions is responsible for implementing those solutions in accordance with the applicable CPs and risk assessments, and registering the solution with NSA.

10. In accordance with CNSS Policy (CNSSP) No. 22, *Policy on Information Assurance Risk Management for National Security Systems* (Reference d), D/As assess and accept risks associated with the implementation of CSfC solutions to protect NSS.

11. Procurement of commercial technologies and systems must comply with CNSSP No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products* (Reference e), which states that all commercial-off-the-shelf IA and IA-enabled products acquired for use on NSS must comply with National Information Assurance Partnership (NIAP) requirements. For those categories of components listed, only products listed on the CSfC Components List may be selected for use in a CSfC solution.

12. USG D/As implementing CSfC solutions must perform a supply chain risk assessment in accordance with the requirements in CNSSD No. 505, *Supply Chain Risk Management (SCRM)* (Reference f).

13. USG D/As implementing CSfC solutions are required to comply with the requirements in the appropriate CP. Implementing a CSfC solution includes:

a. Selecting the components for the CSfC solution from the CSfC Components List, in accordance with the requirements in the CP;

b. Configuring the components according to the configuration requirements in the CP;

c. Testing the CSfC solution per the testing requirements in the CP;

d. Accepting or mitigating the risks associated with the CSfC solution and its integration into the D/A's system;

e. Monitoring the solution in accordance with the CP and reporting incidents;

f. Registering the solutions with NSA; and

g. Obtaining a Registration Acknowledgement Letter from NSA.

14. If a USG D/A requires a solution for which there is no CP, the D/A may work with the NSA to develop a secure solution and receive a National Manager approval letter for that solution. D/As implementing CSfC solutions that deviate from a CP must have that deviation approved by NSA before registering their solution.

15. D/As must register CSfC solutions with the NSA to receive a Registration Acknowledgement Letter. Registration requires the D/A provide architectural diagrams, a completed and signed registration form, a completed compliance matrix, approved deviation letter (if applicable), and any other documentation specified in the CP.

16. D/As implementing CSfC solutions are required to renew those solutions with NSA annually, against the latest CP. D/As renewing against a CP within 90 days of a CP update may register the solution against the previous CP, with the understanding that they will comply with the updated CP when renewing the following year. D/As registering a new CSfC solution must comply with the most recent CP.

17. When a vulnerability is discovered that impacts the residual risk to a CSfC solution, AOs with a registered CSfC solution will receive National Manager Risk Notifications from NSA. The purpose of these notifications is to enable AOs to make informed risk decisions in light of vulnerabilities or potential vulnerabilities in CSfC solutions, to include commercial components used in those solutions. D/As are required to monitor solutions per the requirements in the relevant CSfC CP. D/As must also provide the NSA with incident response information in accordance with the requirements outlined in the CP and National Manager approval letter.

18. If a vulnerability is identified in a CSfC solution requiring immediate mitigation, the NSA will alert D/As implementing these solutions to the presence of the vulnerability and provide appropriate mitigation guidance. Mitigation of these vulnerabilities may require D/As take immediate action to ensure their CSfC solutions are secure.

19. D/As are required to monitor their solutions in accordance with guidance in the CSfC CPs, and must report incidents identified through monitoring to NSA, as described in this advisory and specified in the applicable CPs.

20. D/As with operational CSfC solutions are responsible for reporting incidents involving CSfC solutions to NSA. In addition to the reporting guidance in this advisory,

NSA provides D/As with specific incident reporting guidelines. D/As are required to report any evidence of the following types of CSfC incidents within 24 hours of initial discovery:

a. Spillage or compromise of classified or sensitive information caused by the CSfC solution;

b. Unauthorized user or device accessing an NSS via a CSfC solution;

c. Failure in one or both layers of protection;

d. Malicious access to a CSfC solution;

e. Privilege escalation;

f. Tampering with components;

g. Significant degradation of services for end-user devices (e.g. loss of power, excessive power consumption, battery drain);

h. A security failure in a CSfC component;

i. A solution component sending traffic to unapproved Internet Protocol (IP) address;

j. Unresolved, unexpected inbound or outbound traffic; or

k. Unauthorized and unresolved configuration changes.

21. D/As must maintain physical security for gray network devices consistent with the physical security requirements outlined in the CSfC CPs. D/As are responsible for determining internal procedures for handling gray network devices, within the bounds of the CP requirements. Access to passwords and keys must be restricted accordingly.

22. Individual components of a CSfC solution are subject to security categorization and controls as set forth in CNSS Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* (Reference g).

23. NSA, when designing CSfC solutions, will:

a. Publish CPs and CP risk assessments,

b. Provide National Manager Risk Notifications as necessary to D/As with registered CSfC solutions.

c. Maintain a list of approved commercial products on the CSfC Components List for use as part of a CSfC solution;

d. Maintain a list of CSfC trusted integrators;

e. When informed of an incident involving a CSfC solution, provide mitigation guidance to the affected D/A(s) implementing that solution, as necessary;

f. Notify D/As using registered CSfC solutions of updates to applicable CPs; and

g. Acknowledge registrations and maintain a list of D/As with registered CSfC solutions.

24. Heads of D/As, when implementing CSfC solutions, will:

a. Build, operate, protect, and maintain CSfC solutions in accordance with this advisory and applicable CPs;

b. Obtain approval from NSA for deviations from the CP;

c. Certify and accredit CSfC solutions;

d. Review and understand the risk assessment associated with the CPs; mitigate the risks associated with CSfC solutions;

e. Renew their CSfC solutions with NSA annually, in accordance with paragraph 16 above;

f. Ensure monitoring of CSfC solutions under the CSfC CPs is conducted in accordance with applicable Federal laws and policy, in particular those protecting the privacy rights of U.S. persons; and

g. Report incidents involving CSfC solutions to NSA in accordance with paragraph 20 above.

SECTION VI – DEFINITIONS

25. The following definitions are provided to clarify the use of specific terms contained in this advisory. All other terms used in this issuance are defined in CNSSI No. 4009*, National Information Assurance (IA) Glossary* (Reference h).

a. Black Network: A network in a CSfC solution containing classified information that has been encrypted twice.

b. CSfC: NSA’s business practice for layering commercial technologies to protect classified information on NSS.

c. CSfC Capability Packages (CPs): System-level requirements documents that include architectural diagrams with all of the critical components identified, and a description of the role that each component plays for security. A CP provides requirements for component configuration, solution testing, monitoring, and the use and administration of a CSfC solution. CPs are periodically updated to incorporate new features and best practices.

d. CSfC Components List: List of approved products AOs can choose from for use in approved CSfC solutions. CPs specify which components of the solution must come from the CSfC Components List. To get products on the CSfC Components List, vendors must sign a Memorandum of Agreement with NSA stating that their product will be NIAP validated in a defined period of time, and they will remediate vulnerabilities when discovered.

e. CSfC Trusted Integrator: An organization that is qualified to assemble and integrate components according to a CSfC CP, test the resulting solution, provide a body of evidence to the solution AO, maintain the solution, and be the first line of response in troubleshooting or responding to security incidents.

f. CSfC Risk Assessment: Classified document provided by NSA on the residual risks of fielding a given CSfC solution in accordance with a CP. These risks must be acknowledged and accepted by the AO when the solution is registered with NSA.

g. CSfC Solutions: Layered, NIAP validated commercial technologies to protect NSS that are compliant with a CP and have been registered with NSA.

h. Gray Network: A network in a CSfC solution containing singly-encrypted classified data, as defined in CSfC CPs. Gray network data is controlled unclassified information. One example is the network between the Inner and Outer Virtual Private Network (VPN) Gateways in a VPN solution.

i. Red Network: A network in a CSfC solution containing unencrypted classified information.

SECTION VII – REFERENCES

26. References for this advisory are listed in ANNEX A. Additionally, a list of NSA-approved CSfC Capability Packages (CPs) can be found on NSA's website at http://www.nsa.gov/ia/programs/csfc_program/index.shtml.

Enclosures:
ANNEX A – References
ANNEX B – Acronyms

ANNEX A

REFERENCES

a. CNSS Directive No. 901, *Committee on National Security Systems (CNSS) Issuance System*, dated September 2012.

b. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated July 5, 1990.

c. Executive Order 12333, *United States Intelligence Activities*, dated December 1981, as amended.

d. CNSS Policy No. 22, *Information Assurance Risk Management Policy for National Security Systems*, dated January 2012.

e. CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, dated June 10, 2013.

f. CNSS Directive No. 505, *Supply Chain Risk Management (SCRM)*, dated March 7, 2012.

g. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 27 2014.

h. CNSS Instruction No. 4009, *National Information Assurance (IA) Glossary*, dated April 6, 2015.

i. NSA website, Commercial Solutions for Classified (CSfC) page, located at http://www.nsa.gov/ia/programs/csfc_program/index.shtml.

Note: NSA has developed a CSfC Incident Reporting Guidelines (Version 1.0, dated 18 June 2014) that is available upon request (through an email to csfc@nsa.gov) to USG D/As implementing CSfC solutions.

ANNEX B

ACRONYMS

AO	Authorizing Official
CNSS	Committee on National Security Systems
CNSSAM	Committee on National Security Systems Advisory Memorandum
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CP	Capability Package
CSfC	Commercial Solutions for Classified
CUI	Controlled Unclassified Information
D/A	Department/Agency
IA	Information Assurance
NIAP	National Information Assurance Partnership
NSA	National Security Agency
NSD	National Security Directive
NSS	National Security Systems
SCRM	Supply Chain Risk Management
USG	U.S. Government
VPN	Virtual Private Network