

Committee on National Security Systems

CNSSP No. 7
9 December 2015



POLICY ON THE USE OF COMMERCIAL SOLUTIONS TO PROTECT NATIONAL SECURITY SYSTEMS

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE
FURTHER IMPLEMENTATION



CHAIR

FOREWORD

1. The Committee on National Security Systems (CNSS) is issuing this Policy to direct agencies on how to safeguard National Security Systems (NSS), and the information contained therein, 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 Policy provides a minimum set of security measures required for U.S. Government (USG) Departments and Agencies' (D/As) use of CSfC solutions. For this Policy, 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 classified and unclassified) that transmit, receive, process, or store information using CSfC solutions. D/As must ensure all CSfC solutions comply with NSA requirements, as delineated in this Policy. Implementation of CSfC solutions under this Policy does not preclude the application of additional requirements associated with the security of NSS (e.g., physical security, TEMPEST, Operations Security).

3. This Policy incorporates and supersedes CNSS Advisory Memorandum Information Assurance (IA) 01-15, *Use of Commercial Solutions to Protect National Security Systems* (Reference a), and CNSS Advisory Memorandum IA 01-04, *Information Assurance (IA)—Security Through Product Diversity* (Reference b). This Policy is being issued in accordance with CNSS Directive (CNSSD) No. 901, *Committee on National Security Systems (CNSS) Issuance System*, dated September 2012 (Reference c).

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

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

/s/

Richard Hale

POLICY ON THE USE OF COMMERCIAL SOLUTIONS TO PROTECT NATIONAL SECURITY SYSTEMS

SECTION I – PURPOSE

1. CSfC solutions, when implemented according to the requirements in this Policy, are capable of protecting NSS and the information contained therein. This Policy outlines the requirements for securely implementing CSfC solutions to protect NSS.

SECTION II – AUTHORITY

2. The authority to issue this Policy is derived from National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (Reference d), which outlines the roles and responsibilities for securing NSS, consistent with applicable law, Executive Order 12333, *United States Intelligence Activities*, as amended (Reference e), and other Presidential directives.

3. Nothing in this Policy alters or supersedes the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This Policy applies to all USG D/As 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 – REFERENCES

5. References for this policy 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.

SECTION V – DEFINITIONS

6. The following definitions are provided to clarify the use of specific terms contained in this Policy. All other terms used in this issuance are defined in CNSS Instruction (CNSSI) No. 4009, *Committee on National Security Systems (CNSS) Glossary* (Reference f).

- a. CSfC: NSA's business practice for layering commercial technologies to protect classified information on NSS.
- b. CSfC Capability Packages (CPs): Systems-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. CPs provide 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.
- c. CSfC Components List: List of products D/As can choose from for use in approved CSfC solutions. CPs specify which components of the solution must come from the CSfC Components List.
- d. CSfC Gray Network: A network in a CSfC solution containing classified information that has been encrypted once, as defined in CSfC CPs. One example is the network between the Inner and Outer Virtual Private Network (VPN) Gateways in a VPN solution.
- e. CSfC Risk Assessment: Guidance 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 Authorizing Official (AO) when the solution is registered with NSA.
- f. CSfC Solutions: Layered, National Information Assurance Partnership (NIAP) approved commercial technologies to protect NSS that are compliant with a CP and have been registered with NSA.
- g. 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. D/As may permit Trusted Integrators to perform some or all of the above activities on their behalf, as needed.

SECTION VI – BACKGROUND

7. The USG protects NSS through the use of both NSA-approved CSfC solutions and NSA-certified IA products. Using 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.

8. CSfC solutions employ a layered approach to meet the security requirements necessary to protect NSS. CPs outline a minimum set of requirements for CSfC solutions and provide the implementing D/A with a sufficient level of assurance. NSA also provides a

classified risk assessment associated with each CP. CPs are approved by the National Manager.

9. CSfC solutions differ from NSA-certified IA products in significant ways. The security boundary is different, as CSfC requires two independent layers of encryption. 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 VII – POLICY

10. A CSfC solution that has been approved by the appropriate AO and registered with NSA as being compliant with an NSA-provided CP may be used to protect NSS and the information therein.

11. The NSA shall provide CPs and risk assessments specifying the requirements for the implementation of CSfC solutions and the associated risk. Each D/A using CSfC solutions shall be responsible for implementing those solutions in accordance with the applicable CPs and risk assessments, and registering the solution with NSA. D/As shall assess and accept risks associated with CSfC solutions prior to implementing those solutions on NSS. D/As shall also ensure that contractors implementing CSfC solutions do so in accordance with applicable CPs and the requirements of this Policy.

12. Procurement of commercial technologies and systems shall comply with CNSSP No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products* (Reference g), which states that all commercial-off-the-shelf IA and IA-enabled products acquired for use on NSS shall comply with 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.

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

14. CSfC solutions must 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 NSS;
- e. Monitoring the solution in accordance with the CP;
- f. Registering the solutions with NSA; and
- g. Obtaining a Registration Acknowledgement Letter from NSA.

15. If a USG D/A requires a solution for which there is no CP, the D/A must work with the NSA to develop a secure solution and receive a National Manager approval letter for that solution.

16. CSfC solutions that deviate from a CP must have that deviation approved by the NSA before registering their solution.

17. 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 checklist, approved deviation letter (if applicable), and any other documentation specified in the CP.

18. D/As implementing CSfC solutions must 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 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.

19. When a vulnerability is discovered that increases 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.

20. If a vulnerability identified in a CSfC solution requires immediate mitigation, the NSA shall 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 provide the necessary level of protection.

21. D/As with operational CSfC solutions are responsible for monitoring their solutions in accordance with guidance in the CSfC CPs, and reporting incidents involving CSfC solutions to NSA. In addition to the reporting guidance in this Policy, NSA provides D/As implementing CSfC solutions with specific incident reporting guidelines. D/As shall report any evidence of the following types of incidents, if they are caused by or related to the CSfC solution, within 24 hours of initial discovery:

- a. Spillage or compromise of classified information;

- b. Unauthorized user or device accessing an NSS;
- c. Failure in one or both layers of encryption;
- d. Malicious access to a CSfC solution;
- e. Privilege escalation;
- f. Tampering with CSfC 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 or addresses;
- j. Unresolved, unexpected inbound or outbound traffic; or
- k. Unauthorized and/or unresolved configuration changes.

22. D/As shall 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.

23. Configuration of a CSfC layered solution requires manufacturer diversity in the selection of CSfC components. D/As (and CSfC Trusted Integrators) shall not use single-manufacturer implementations of both layers of encryption in a CSfC solution, unless explicitly permitted in the applicable CP, or unless the following conditions are met:

- a. The manufacturer demonstrates sufficient independence in the code base and cryptographic implementations of the products used to implement each layer. To demonstrate the independence of each layer, the manufacturer documents the similarities and differences between the two products, to include cryptographic hardware components, software code base (i.e., operating system), software cryptographic libraries, and development teams;
- b. The vendor documents measures taken to ensure the supply chain risk is no greater than would be the case for products from two different vendors; and
- c. NSA reviews the documentation provided by the vendor, and determines the manufacturer's solution provides the necessary security for each layer.

24. D/As may consult with CSfC trusted integrators for assistance with the assembly, testing, and/or maintenance of CSfC solutions. NSA shall assess potential trusted integrators to ensure that they pose no threat to the security of CSfC solutions.

25. CSfC components that have processed unencrypted classified information must be sanitized or destroyed upon reaching end of life, using one of the processes described in the *NSA/CSS Storage Device Sanitization Manual* (Reference i).

SECTION VIII – RESPONSIBILITIES

26. NSA shall:

- a. Approve and publish CPs and 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.

27. Heads of D/As, or their designees, shall, when implementing CSfC solutions:

- a. Build, authorize, operate, protect, assess, and maintain CSfC solutions in accordance with this Policy and applicable CPs;
- b. Obtain approval from NSA for deviations from the CP;
- c. Review and understand the risk assessment associated with the CPs; mitigate the risks associated with CSfC solutions;
- d. Register their CSfC solutions with NSA, and renew them annually, in accordance with paragraph 18 above;
- e. 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;
- f. Report incidents involving CSfC solutions to NSA in accordance with paragraph 21 above; and

- g. Sanitize or destroy classified devices upon reaching end of life, in accordance with paragraph 25 above.

Enclosures:

ANNEX A – References

ANNEX B – Acronyms

ANNEX A**REFERENCES**

- a. CNSS Advisory Memorandum IA 01-15, *Use of Commercial Solutions to Protect National Security Systems*, dated April 2015 (hereby superseded).
- b. CNSS Advisory Memorandum IA 01-04, *Information Assurance (IA)—Security Through Product Diversity*, dated July 2004 (hereby superseded).
- c. CNSS Directive No. 901, *Committee on National Security Systems (CNSS) Issuance System*, dated September 2012.
- d. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated 5 July 1990.
- e. Executive Order 12333, *United States Intelligence Activities*, dated December 1981, as amended.
- f. CNSS Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, dated 6 April 2015.
- g. CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, dated 10 June 2013.
- h. CNSS Directive No. 505, *Supply Chain Risk Management (SCRM)*, dated 7 March 2012.
- i. NSA/CSS Policy Manual 9-12, *NSA/CSS Storage Device Sanitization Manual*, dated 15 December 2014 (located at: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml).
- j. 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. In addition, the NSA website includes links to the CSfC CPs and related information (e.g., registration form, compliance checklist, components list).

ANNEX B**ACRONYMS**

AO	Authorizing Official
CNSS	Committee on National Security Systems
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
D/A	Department/Agency
IA	Information Assurance
IP	Internet Protocol
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