Committee on National Security Systems

CNSSP 32
May 2022

POLICY ON CLOUD SECURITY

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

CHAIR

FOREWORD

1. This document establishes the Policy on Cloud Security for National Security Systems (NSS). The Committee on National Security Systems is issuing this policy to establish minimum security requirements for cloud computing services. Cloud computing refers to ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing enables Departments and Agencies to consolidate infrastructure, leverage commodity Information Technology (IT) functions, and eliminate functional redundancies while improving continuity of operations. A minimum baseline of security controls for NSS ensures the protection of sensitive data while enabling mission effectiveness.

2. This policy derives its authority from *National Security Directive 42,* which outlines the roles and responsibilities for securing NSS, and applicable sections of the Federal Information Security Management Act of 2002.

3. This policy also supports Executive Order 14028, *Improving the Nation's Cybersecurity*, 12 May 2021, the corresponding National Security Memorandum (NSM-8), *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems,* 19 January 2022, and National Manager Memorandum (NMM-2022-01).

4. This policy is available from the CNSS Secretariat, as noted below, or the CNSS website: https://www.cnss.gov.

MARK G. HAKUN

CNSS Secretariat. National Security Agency. 9800 Savage Road, STE 6747. Ft Meade, MD 20755-6747
Office: (410) 854-6805
CNSS@nsa.gov

Table of Contents

CLOUD SECURITY FOR NATIONAL SECURITY SYSTEMS

SECTION I—PURPOSE

1. This document establishes the minimum security requirements for National Security Systems (NSS) migrating to or operating in a cloud environment. For this policy, the term U.S. Government Executive Departments and Agencies (D/As), shall be interpreted to include Federal bureaus and offices. This policy establishes requirements for a common approach to the use of NSS in various cloud environments.

SECTION II—AUTHORITY

2. The authority to issue this policy derives from *National Security Directive 42*, which outlines the roles and responsibilities for securing NSS, consistent with applicable law, E.O. 12333, as amended, and other Presidential directives.

3. Nothing in this policy shall alter or supersede the authorities of the Director of National Intelligence.

SECTION III—SCOPE

4. This policy applies to all D/As that own or operate NSS, including supporting contractors that operate, use, or manage NSS.

SECTION IV—POLICY

5. This Policy provides the minimum security requirements for operating NSS in a cloud environment.

6. NSS owners are responsible for ensuring that all CNSS and other federal requirements are implemented in their systems. Commercial Cloud Service Providers (CSPs) may be leveraged in order to meet these requirements. Tools such as Customer Responsibility Matrices or other similar documentation that articulates the roles and responsibilities for implementers should be leveraged to ensure that all requirements are addressed.

7. There are multiple service offerings by CSPs, including Infrastructure as a Service, Platform as a Service, and Software as a Service. The NSS owner is responsible for identifying the applicable security requirements and verifying that the requirements are met by the CSP and

the NSS. Cloud authorization processes, such as the FedRAMP program, can assist the NSS owner by providing a body of evidence to validate requirements implementation as well as continuous monitoring to ensure that those requirements continue to be met.

8. NSS owners must ensure the categorization and the classification level of the NSS system is appropriate and supported by the CSP, and that information within the NSS system is stored, processed, and transmitted in accordance with the security requirements in CNSS Instruction (CNSSI) 1253.

9. Cloud environments must comply with the security controls identified in CNSSI 1253 and any additional issuances as appropriate. Furthermore, Cloud instantiations must implement strong authentication.

10. For IT services external to the D/As and provided by a commercial entity, security requirements must be clearly defined in contracts for cloud computing services. The following security requirements enable strong authentication to systems in a cloud:

a. NSS that are leveraging commercial cloud environments must comply with CNSS security requirements.

b. D/As must develop cloud cybersecurity policies and procedures that establish D/A policies and processes for cloud based systems including policies on acquisition, secure development, secure configuration, and system sustainment. This guidance must include minimum security requirements.

c. For unclassified NSS, the minimum requirements must be equivalent to the FedRAMP High baseline.

d. NSS cloud environments must either be physically separated from all non-Federal tenant systems and infrastructures, or must have the cryptographic (virtual) separation validated or approved by NSA.

e. All NSS data must remain under U.S. jurisdiction or in U.S. Territories or geographic locations where there is U.S. jurisdiction.

f. Data spill security processes and procedures must be clearly defined and addressed in service level agreements with the CSP.

g. The NSS system owner must ensure the CSP maintains, patches, monitors, and protects the infrastructure, operating systems, and applications supporting all service offerings; and receives, acts upon, and reports compliance with NSS Binding Operational Directives and Emergency Directives, as applicable.

h. When implementing classified cloud services, the CSP and NSS system owner must comply with the requirements of EO 13526, *Classified National Security Information* and the *National Industrial Security Program Operating Manual (NISPOM)*.

i. Report cyber incidents to D/As following procedures in CNSSI No. 1010, *Cyber Incident Response*.

11. NSS cloud environments shall adopt Zero Trust Architecture concepts for enhanced security.

SECTION V—RESPONSIBILITIES

12. The heads of each Federal department or agency shall ensure the implementation of this policy and develop clear and comprehensive implementation guidance in support of current law, policies, regulations, and business rules.

13. The CNSS will provide guidance to the D/As on cloud security and best practices applicable to NSS.

SECTION VI—DEFINITIONS

14. 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 No. 4009, *Committee on National Security Systems Glossary*.

a. Cloud Service Provider means a person, organization, or entity responsible for making a service available to service consumers.

b. Infrastructure as a Service (IaaS) means the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

c. Platform as a Service (PaaS) means the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

d. Software as a Service (SaaS) means the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

SECTION VII —REFERENCES

15. Future updates to referenced documents shall be considered applicable to this policy. References for this Policy are contained in Annex A.

Enclosure:
ANNEX A - References

ANNEX A

REFERENCES

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

2. Federal Information Security Management Act of 2002

3. Executive Order 13526, *Classified National Security Information*, December 29, 2009

4. Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021.

5. National Security Memorandum 8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*, January 19, 2022.

6. Committee for National Security Systems Instruction Number 1010 (CNSSI No. 1010), *Cyber Incident Response*, September 27, 2021.

7. Committee for National Security Systems Instruction Number 1253 (CNSSI No. 1253), *Categorization and Control Selection for National Security Systems*, March 27, 2014.

8. Committee for National Security Systems Instruction Number 4009 (CNSSI 4009), *Committee on National Security Systems Glossary*, March 2, 2022

9. National Industrial Security Program Operating Manual (NISPOM), December 21, 2020.

10. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*, September 2011