



DEPARTMENT OF THE NAVY  
UNITED STATES NAVAL ACADEMY  
121 BLAKE ROAD  
ANNAPOLIS MARYLAND 21402-1300

USNAINST 8510.03  
28/ITSD  
25 Apr 2016

USNA INSTRUCTION 8510.03

From: Superintendent, United States Naval Academy

Subj: ACQUISITION AND USE OF CLOUD SERVICES

- Ref:
- (a) USNAINST 8510.01, Cybersecurity Risk Management
  - (b) USNAINST 5230.1A, Information Technology and Cybersecurity Policy and Standards
  - (c) Department of the Navy Deputy Chief Information Officer Memorandum, Ser N2N6BC/5U120231, Interim Guidance and Governance For Acquisition and Use of Navy Commercial Cloud Computing Services, 9 Nov 2015
  - (d) DoD Directive 5230.09, Clearance of DoD Information for Public Release, 22 Aug 2008
  - (e) DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release, 13 Aug 2014
  - (f) Department of the Navy Chief Information Officer Memorandum, Acquisition and Use of Commercial Cloud Computing Services, 15 May 2015
  - (g) USNAINST 5211.3C, USNA Privacy Program

- Encl:
- (1) Cloud Service Request
  - (2) Definitions

1. Purpose. Per references (a) through (g), this instruction is issued to establish policy on acquiring and using cloud services in support of the United States Naval Academy (USNA) mission.

2. Background. Cybersecurity controls are applied to the USNA mission network to protect sensitive data within the network authorization boundary. Information technology services external to this boundary that are provided by a Cloud Service Provider (CSP) must have risk-appropriate confidentiality and integrity protections. Cloud services also have a network and client support impact that must be assessed before being authorized.

### 3. Definitions

a. Software as a Service (SaaS): A software delivery model where the software and the associated data is hosted in a cloud environment by a third party. Typically, the user accesses the software on demand using a browser on a computer or mobile device.

b. Platform as a Service (PaaS): A software delivery model where a CSP provides an online software development platform. Developers use the CSP's computing environments, tools, and libraries to create, test, manage, and host software applications.

c. Infrastructure as a Service (IaaS). A software delivery model where a CSP provides the necessary hardware and software upon which a customized computing environment can be built. The CSP provides an unmanaged environment that can be customized, or provides pre-configured virtual machines on which an application can be installed.

4. Actions and Responsibilities. This policy applies to any cloud service used by the enterprise, a cost center, a sub-cost center, an office, a group of individuals, or a single individual. This policy applies to all types of cloud services: SaaS, PaaS, and IaaS; legacy and future.

### 5. Policy

a. Per reference (a), all cloud services shall be managed with respect to cybersecurity risk.

b. Use of cloud services is not authorized for storing, processing, transmitting, or displaying classified information.

c. Cloud services shall not be acquired for purposes that do not support the USNA mission.

d. Cloud services accessed from the USNA government mission network for personal use is prohibited except as authorized per reference (b).

e. The USNA Configuration Control Board (CCB) must approve acquisition and all use of cloud services. The data owner shall provide a justification, information security determination, and impact assessment for each request to acquire or use a cloud service by submitting enclosure (1) to the CCB. The data owner is responsible for ascertaining and documenting that the requested cloud service meets the required security level for the type of information to be stored or transmitted.

f. Acquisition for cloud services to support an enterprise requirement must follow guidance promulgated in reference (c). These requirements might also apply to a cloud service acquisition supporting a more restricted use as determined by the CCB.

g. References (d) and (e) establish policy associated with reviewing DoD information for public release. The provisions of these references, as they pertain to USNA, are summarized as follows:

(1) All USNA employees are considered DoD personnel. This includes faculty and foreign nationals, military assigned to USNA, including reservists, as well as employees of Non-Appropriated Fund (NAF) activities. Employees of non-DoD activities that use the USNA network (e.g., The Naval Academy Athletic Association) fall within this definition for the purposes of cloud security risk management.

(2) Official DoD information is all information acquired by DoD personnel as part of their official duties.

(3) Official DoD information intended for public release that does not pertain to military matters, national security issues, or subjects of significant concern to the DoD, does not require a security and policy review before release.

(4) Academic information that is not intended for release outside of USNA does not require a security and policy review.

(5) Controlled Unclassified Information (CUI) may not be publicly released.

h. A CSP must provide security to the level specified in reference (f) if the CSP is used to store or transmit sensitive data.

6. User Responsibility. For all cloud services authorized by the CCB:

a. Users will comply with all vendor terms and conditions.

b. The data owners will notify the CCB when cloud services are no longer needed.

c. The data owner shall conduct and report the results of periodic audits of CUI as required by reference (g):

(1) If CUI storage is not authorized, the audit is to discover and remove CUI.

(2) If CUI storage is authorized, the audit is to validate the continued need for storing CUI and minimize the volume.

7. USNA Service Level Agreement

a. Unless otherwise excepted, USNA will support authorized cloud SaaS applications to the same extent as commensurate with internally hosted applications. No support will be provided for PaaS and IaaS. No support will be provided when government resources are used to store or access personal data in the cloud when authorized by reference (b).

b. USNA does not guarantee that cloud services will remain available when accessed internally from a USNA network.

c. USNA may block access to cloud services if necessary to obviate or mitigate cybersecurity risk.

d. USNA may allocate network bandwidth used to access the CSP to higher priority USNA mission requirements as necessary.

  
W. E. CARTER, JR

Distribution:  
Non Mids (electronically)

CLOUD SERVICE REQUEST

1. Description. State the name of the person making the request and the data owner, describe the information to be stored or transmitted, identify the CSP and the requested service, and indicate whether the request is for SaaS, PaaS, and/or IaaS.

2. Justification. Describe how the cloud service will be used and why internal USNA resources and/or locally hosted applications are inadequate.

3. Information security. The data owner is responsible for ascertaining and documenting that the requested cloud service satisfies the required security level for the type of information to be stored or transmitted.

a. Specify one or more information types:

- Public
- Limited Access
- Export Controlled
- Privacy Information
- Protected Health Information
- Payment Card Industry Data
- Other

b. Identify the highest required security level based on the information type per reference (f):

- Security review not required per references (d) and (e) (public information ONLY).
- Level 2
- Level 4
- Level 5

c. List the information security standards which this CSP provides for the requested cloud service (obtain this information from the vendor). Examples: HIPAA, PCI DSS, ITAR, FIPS 140-2, FISMA, FedRAMP, etc.

d. The CSP provides acceptable security for the information to be stored or transmitted:  Yes  No

4. Impact. Assess and report the impact associated with use of the cloud service:

a. Network (MBps, obtain this information from the vendor where possible):

b. Use profile (e.g., continuous, intermittent, 8 hrs/day, M-F, 3x per semester, etc):

5. Submitted:

## DEFINITIONS

### Cloud service types:

Software as a Service (SaaS): A software delivery model where the software and the associated data is hosted in a cloud environment by a third party. Typically, the user accesses the software on demand using a browser on a computer or mobile device.

Platform as a Service (PaaS): A software delivery model where a CSP provides an online software development platform. Developers use the CSP's computing environments, tools, and libraries to create, test, manage, and host software applications.

Infrastructure as a Service (IaaS): A software delivery model where a CSP provides the necessary hardware and software upon which a customized computing environment can be built. The CSP provides an unmanaged environment that can be customized, or provides pre-configured virtual machines (VMs) on which application can be installed.

### Information types:

Public: Information that is intended for unrestricted public dissemination.

Limited Access Information: Information that is not Controlled Unclassified Information (CUI, see below), but data for which the owner requires more limited access than full public release.

Controlled Unclassified Information: This is the categorical designation that refers to unclassified information that under law or policy requires protection from unauthorized disclosure as established by Executive Order 13556 (Nov 2010). Designating information as CUI is the responsibility of the owning organization. CUI contains a number of categories, including:

Export Control: Unclassified information concerning certain items (including dual use items), commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives; items identified in export

administration regulations; international traffic in arms regulations and the munitions list; and sensitive nuclear technology information.

Privacy: Refers to personal information or personally identifiable information (PII) as defined in Office of Management and Budget (OMB) M-07-16, or means of identification as defined in 18 USC 1028(d)(7).

Protected Health Information as defined in the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191).

Payment Card Industry Data: Refers to information contained on a customer's payment card. Only the primary account number, expiration date, service code, and cardholder name may be stored. The data is printed on either side of the card and is contained in digital format on an embedded magnetic stripe.

Other: Information requiring explicit CUI special handling designation; for example, For Official Use Only, and Law Enforcement Sensitive. Designating information as CUI is the responsibility of the owning organization.

Security levels, from reference (f):

Level 2 (Non-controlled Unclassified Information: Public and Limited Access Information). Data cleared for public release as well as unclassified information not designated as CUI but which requires some level of access control.

Level 4 (Controlled Unclassified Information). Unclassified information that under law or policy requires protection from unauthorized disclosure.

Level 5. Controlled Unclassified Information that requires a higher level of protection as deemed necessary by the information owner, public law, or other government regulations.