

**Department of Homeland Security
Cybersecurity and Infrastructure
Security Agency
Emergency Communications Division**



**Communications Asset Survey
and Mapping (CASM) Tool**

Rules of Behavior

(End-User)

11/2/2020

DOCUMENT CHANGE HISTORY

Version	Date	Author	Description
1.0	4/1/2015	J Pollard	Initial Draft
2.0	5/1/2015	J Pollard	Review Updates
3.0	1/10/2018	J Pollard	Review Updates
4.0	7/30/19	J Pollard	Reviewed
5.0	5/15/20	J Pollard	Updates for Two-Factor Authentication
6.0	11/2/20	J Pollard	Update to identify Organizational Users

Table of Contents

- 1.0 INTRODUCTION 4
- 2.0 REFERENCES 4
- 3.0 CASM RULES OF BEHAVIOR..... 4
 - 3.1 System Access 5
 - 3.2 Access Control Measures 5
 - 3.3 Data Protection 6
 - 3.4 Incident Reporting..... 7
 - 3.5 Accountability..... 7

1.0 INTRODUCTION

Rules of behavior that apply to access and use of Department of Homeland Security (DHS) information technology (IT) resources are a vital part of the DHS IT Security Program and help to ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.

The purpose of DHS Rules of Behavior (ROB) is to inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS systems and using DHS IT resources capable of accessing, storing, receiving, or transmitting sensitive information. The DHS End User Rules of Behavior apply to every user of the CASM system.

These Rules of Behavior are consistent with the IT security policy and procedures given by DHS Management Directive 140-1, "Information Technology Systems Security", "DHS Sensitive Systems Policy Directive 4300A," and the "DHS 4300A Sensitive Systems Handbook."

Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

The Communication Assets Survey and Mapping (CASM) system is operated and maintained by the DHS Cybersecurity and Infrastructure Security Agency's Emergency Communications Division.

An Organizational User is defined as a CASM user who is a DHS employee or contractor. An Organizational User Account is a CASM Account providing access for an Organizational User to conduct DHS tasking.

2.0 REFERENCES

- a) DHS Sensitive Systems Policy Directive 4300A v13, June 27, 2017
- b) DHS 4300A Sensitive Systems Handbook v12.0, November 15, 2015
- c) DHS Information Security Continuous Monitoring Strategy, An Enterprise View, May 14, 2014
- d) DHS Directive MD Number: 140-01, Revision Number: 00, Information Technology Systems Security, 07/31/2007

3.0 CASM RULES OF BEHAVIOR

The following rules of behavior apply to all users who use the CASM system. DHS Rules of Behavior apply to users at their primary workplace, while teleworking or at a satellite site, at any alternative workplaces, and while traveling.

3.1 System Access

- I understand that I am given access only to those systems to which I require access in the performance of my official duties.
- I will not attempt to access systems I am not authorized to access.
- I understand that I have no expectation of privacy when accessing the CASM system and that I acknowledge DHS's right to monitor system use.
- I will notify the CASM Help Desk, casmhelp@cisa.dhs.gov, under any circumstances in which I no longer require access to the CASM system.

3.2 Access Control Measures

The CASM system requires two-factor authentication (2FA) of the user's identity for access. Two-factor authentication may be provided through the use of either of two methods:

Method A: a DHS Personal Identity Verification (PIV) card OR Department of Defense Common Access Card (CAC). Users who have gained access using Method B, below, may associate their PIV card or CAC to their account from within the CASM system My Account menu. Once associated, they may use their PIV card or CAC certificates for all future access. Organizational Users are restricted to this Method for access to the system.

Method B: a combination of user credentials (user-id/password) and entering a CASM-generated security code received on a device capable of receiving SMS messages.

A new user must use the system provided user-id and temporary password, enter a 2FA phone number to receive the CASM-generated security code, enter the received code then change the password to one only they know, set their personal Security Questions/Answers and Acknowledge this ROB.

With regard to the above defined access methods:

- I will choose passwords that are at least eight characters in length. Your password may include upper and lower case letters, numerals, and special characters. Your password must not contain two or more spaces in a row.
- I will protect passwords from disclosure.
- I will not share passwords.
- I will not provide my password to anyone, including system administrators.
- I will not record passwords on paper or in electronic form, and I will not store them on or with workstations, laptop computers, or other electronic devices.
- To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.

- While passwords do not expire, I will promptly change a password whenever its compromise is known or suspected to have occurred.
- I will not attempt to bypass access control measures
- I will not redirect SMS messages used for access authentication.
- I will not store a Personal Identity Verification (PIV) card with workstations, laptop computers, or PEDs. I will keep antivirus and firewall software on my computer equipment and mobile devices up to date.
- I will not program computer equipment or mobile devices with sign-on sequences, passwords, or access phone numbers.
- If I am an Organizational User, I will only use an Organizational User Account to conduct DHS tasking.
- I understand that laptop computers used to access CASM shall be powered down when not in use (due to volatile memory vulnerabilities).

3.3 Data Protection

- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I understand that media containing data extracted from the CASM system (print or electronic) is required to be labeled as FOUO and protected accordingly (i.e. maintained in locked cabinets, desks, offices etc.) when unattended. All printing of sensitive documents shall occur only when a trusted person is attending the printer.
- I understand that data extracted from the CASM system cannot be introduced into any other system (e.g., sent via email, posted on social media etc.)
- I understand that data CASM containing PII or data downloaded to my mobile device or laptop must be protected using FIPS 197 (AES 256 bit) encryption implemented by cryptographic modules that are FIPS 140-2 validated, and that mobile computing devices must be powered down when not in use (due to volatile memory vulnerabilities).
- I understand that digital and non-digital CASM media to be disposed of, reused, or released from organizational control, will be sanitized using an approved NSA method as listed on https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.
- I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I am away from my work area, even for a short time. I will log off when I leave for the day.
- Downloaded CASM reports or ad-hoc extracts shall be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period.
- I agree to abide by software copyrights and to comply with the terms of all licenses used by the CASM system.

3.4 Incident Reporting

- I will promptly report suspected IT security incidents to the CASM DHS Help Desk at casmhelp@cisa.dhs.gov. Users can report cyber security incidents and observed vulnerabilities 24/7 through the DHS website to the United States Computer Security Emergency Readiness Team (US-CERT) at <https://www.us-cert.gov/report>.

3.5 Accountability

- I understand that I have no expectation of privacy while using any DHS CASM systems
- I understand that I will be held accountable for my actions while accessing and using the DHS CASM systems and related DHS IT resources.