

UNCLASSIFIED



United States Cyber Command Manual (USCCM)

OPR: J9/OCIO
DISTRIBUTION: A

USCCM 5200-08 Vol III
25 January 2019

Cybersecurity Manual: Volume III - Information Systems Audit Implementation

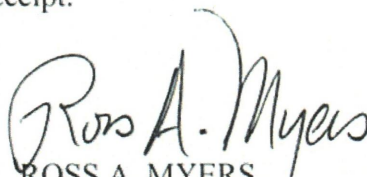
1. Purpose. This USCCM expands upon United States Cyber Command Instruction (USCCI) 5200-08, *Cybersecurity*. It implements Department of Defense Instruction (DODI) 8500.01, *Cybersecurity*, National Institute of Standards and Technology (NIST) and United States Cyber Command (USCYBERCOM) requirements for auditing activity on Command information systems (IS). Auditing is critical for detecting and addressing insider threats and other malevolent activity on Command systems. An audit is the independent review and examination of records and activities to assess the adequacy of system controls to ensure compliance with established policies and operational procedures. Compliance with this document is mandatory.
2. Supersedes/Cancellation. This manual replaces audit guidance in USCCI 5200-08, *Cybersecurity Policy*, dated 8 December 2016.
3. Applicability. This Manual applies to all personnel assigned or attached (military, civilian and contractor) to USCYBERCOM. Nothing in this manual will alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information or Special Access Programs.
4. Responsibilities. Responsibilities are outlined in Enclosure 1.
5. Procedures. Procedures are outlined in Enclosure 2.
6. Releasability. Cleared for Public Release. This Manual is approved for public release; distribution is unlimited. Department of Defense (DOD) Components, other Federal agencies, and the public may obtain copies of this directive.

UNCLASSIFIED

UNCLASSIFIED

USCCM 5200-08 Vol III

7. Effective Date. This Manual is effective upon receipt.


ROSS A. MYERS
Rear Admiral, U.S. Navy
Chief of Staff

Enclosures:

Enclosure 1 – Roles and Responsibilities

Enclosure 2 – Procedures

Attachment 1 – Glossary of References and Supporting Information

UNCLASSIFIED

ENCLOSURE 1

1. Roles and Responsibilities. The following are specific to auditing Command IS and are in addition to the responsibilities identified in USCCI 5200-08.

1.1. All Directorates. Report any suspicious IS behavior or activity in accordance with (IAW) instructions on the USCYBERCOM home page on the National Security Agency Network (NSANet) under "Incident Reporting."¹

1.2. Chief Information Officer (CIO)/ Deputy CIO (DCIO).

1.2.1. Plan, implement and manage automated audit management activities for Command IS in consultation with legal counsel and civil liberties and privacy officials.

1.2.2. Ensure implementation of audit functions pursuant to requirements in this manual.

1.2.2. Ensure personnel assigned to perform audit tasks in this Manual are trained and qualified to perform the duties.

1.2.3. Ensure automated audit management capabilities are integrated with Command continuous monitoring efforts.

1.3. Information System Owner (ISO).

1.3.1. Ensures cybersecurity personnel administering access control functions do NOT also administer audit functions.

1.3.2. Ensures IS under their purview implement the audit requirements included in this policy.

1.3.3. Ensures network-connected IS transmit audit logs to the Command audit data repository.

1.3.4. Ensures standalone enclave IS store audit logs to a centralized enclave audit data repository.

1.3.5. Ensures the retention of additional audit data not directly addressed in this policy as needed and as permitted by all applicable laws, regulations, policies and procedures.

1.4. Authorizing Official (AO) or Authorizing Official Designated Representative (AODR).

1.4.1. Tailors the auditing requirements outlined in this policy, as required for specific systems, IAW a risk assessment.

1.4.2. Ensures a list of auditable events and activities, details and information elements for auditable events and activities, review frequency and any adjustment to the auditing requirements are documented within the System Security Plan (SSP).

1.5. Information System Security Engineers (ISSE).

1.5.1. Ensure Command ISs are designed to include auditing capabilities as described in this Manual.

¹ [https://uscybercom.sp.web.nsa.ic.gov/sites/Cybernet/ig/SitePages/Incident Reporting Form.aspx](https://uscybercom.sp.web.nsa.ic.gov/sites/Cybernet/ig/SitePages/Incident%20Reporting%20Form.aspx)

1.5.2. Consult with legal counsel and civil liberties and privacy officials to ensure audit data is created and handled in compliance with applicable civil liberties and privacy laws and regulations.

1.6. Information System Security Managers (ISSM). Ensure all Command IS automatically create audit logs of all access activities and the logs are reviewed at least weekly.

1.7. Information System Security Officers (ISSO).

1.7.1. Review and analyze audit data that has been reduced by the Command security event audit reduction tool at least weekly and take appropriate actions as necessary IAW current procedures;

1.7.2. Document requirements for auditable events and activities, details and information elements for auditable events and activities, and review frequency within the SSP, including AO approved exceptions.

1.7.3. Increase the level of audit review, analysis and reporting when directed.

1.7.4. Ensure data is handled in compliance with applicable civil liberties and privacy laws and regulations.

1.8. Systems Administrators.

1.8.1. Configure logging on individual systems and network devices to capture data required by this Manual.

1.8.2. Monitor system logging activity to ensure logging functions are working properly. Take action to correct malfunctions quickly.

1.8.3. Assist incident response personnel by providing audit log information as required during incident investigations.

ENCLOSURE 2**2. Procedures.**

2.1. **Use.** Use audit records for individual accountability, reconstruction of events, intrusion detection and problem identification.

2.2. **Contents of Audit Records.** An audit record includes sufficient information to establish what activities occurred and who (or what) caused them. Document audited events in the appropriate SSP or baseline configuration document for the operating system, network device, or application. Collect and report all logs of activities in Zulu time to ensure a standardized date/time stamp. Generate audit records for the following events:

2.2.1. Authentication Events:

- Logons (Success/Failure)
- Logoffs (Success/Failure)

2.2.2. File and Objects Events:

- Create (Success/Failure)
- Access (Success/Failure)
- Delete (Success/Failure)
- Modify (Success/Failure)
- Permission Modification (Success/Failure)
- Ownership Modification (Success/Failure)

2.2.3. Writes/downloads to external devices/media (e.g., A: Drive, CD/DVD devices/printers) (Success/Failure).

2.2.4. Uploads from external devices (e.g., CD/DVD drives) (Success/Failure).

2.2.5. User and Group Management Events:

- User add, delete, modify, suspend and lock (Success/Failure)
- Group/Role add, delete and modify (Success/Failure)

2.2.6. Use of Privileged/Special Rights Events:

- Security or audit policy changes (Success/Failure)
- Configuration changes (Success/Failure)
- Admin or root-level access (Success/Failure)
- Privilege/Role escalation (Success/Failure)
- Direct access attempts (Success/Failure)
- Audit and log data accesses (Success/Failure)
- System reboot, restart and shutdown (Success/Failure)
- Print to a device (Success/Failure)
- Print to a file (e.g., .pdf format) (Success/Failure)
- Application initiation (e.g., Firefox, Internet Explorer, Microsoft Office Suite, etc.) (Success/Failure)

- Export of information (e.g., from CD-RW, thumb drives, or remote systems) (Success/Failure)
- Import of information (e.g., from CD-RW, thumb drives, or remote systems) (Success/Failure)

2.2.7. Concurrent logons from different workstations (Success/Failure).

2.2.8. Queries (e.g., human-generated, machine generated).

2.3. Audit records must contain sufficient information to establish, at a minimum:

2.3.1. The type of event.

2.3.2. The date and time the event occurred.

2.3.3. The location or device where the event occurred.

2.3.4. The source of the event.

2.3.5. The outcome (success or failure) of the event.

2.3.6. The identity of any user/subject associated with the event.

2.4. **Audit Record Security.** Protect audit records from unauthorized access. Take the following precautions:

2.4.1. Strictly control access to online audit logs.

2.4.2. Ensure separation of duties between security personnel who administer the access control function from those who administer the audit record.

2.4.3. Ensure confidentiality of audit record information.

2.4.4. Protect audit logs from accidental or malicious deletion, tampering and/or modification.

2.4.5. Distribute paper copies of audit logs only on a strict need-to-know basis and destroy when no longer needed.

2.5. **Audit Record Review.** Review audit records for unauthorized activity at least weekly. Use an approved automated audit reduction tool to reduce the volume of audit data to facilitate manual review. Logging and review requirements may change with increase in Cyberspace Protection Conditions (CPCON), including more frequent reviews, focused string searches, analysis of activity below normal trigger thresholds, and submission of logs to an organization designated to conduct specialized reviews. Document any findings in an audit report. Include, as a minimum, a description of the finding, factual details that led to the finding and recommendations, as appropriate. Review audit records:

2.5.1. Following a known system or application software problem, a known violation of existing policy by a user, or anomalous or suspicious activity.

2.5.2. For indications of initialization sequence errors and log on errors.

2.5.3. For indications of inappropriate or unusual system processes.

2.5.4. For anomalies regarding system performance or resource utilization.

2.5.5. For unusual network traffic, excessive bandwidth utilization rates, and alerts notifications from border defense devices.

2.5.6. For any other suspicious activity or suspected violations.

2.6. **Reporting.** Report any suspicious IS behavior or activity IAW instructions on the USCYBERCOM home page on NSANet under "Incident Reporting."

2.7. **Audit Storage.** Store all audit logs in a secured tamper-resistant, adequately sized repository with controlled access to ensure no loss occurs.

2.8. **Record Copy.** Backup and maintain the record copy of the audit data collected IAW USCCI 5000-05, *Records Management Program*.

ATTACHMENT 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

18 United States Code (U.S.C.) §2510, *Electronic Communications Privacy Act (ECPA)*, 21 October 1986

NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 22 January 2015

CNSSI 1015, *Enterprise Audit Management Instruction for National Security Systems*, September 2013

CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*, 6 April 2015

DOD 8570-01M, *Information Assurance Workforce Improvement Program*, Incorporating Change 4, 10 November 2015

DODI 8500.01, *Cybersecurity*, 14 March 2014

CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*, 09 February 2011, Current as of 09 June 2015

CJCSM 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

USCCI 5000-05, *Records Management Program*, 8 January 2018

USCCI 5200-08, *Cybersecurity*, 12 December 2018

NSA/CSS Policy Instruction 6-0007, *Collection, Reduction, and Retention of Audit Data for NSA/CSS Information Systems*, 04 February 2016, Revised 04 January 2017

Acronyms

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
CIO	Chief Information Officer
CPCON	Cyberspace Protection Conditions
DCIO	Deputy Chief Information Officer
DOD	Department of Defense
DODI	Department of Defense Instruction
IAW	in accordance with
IS	Information System
ISO	Information System Owner
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
NSA/CSS	National Security Agency/Central Security Service
NSANet	National Security Agency Network
OCIO	Office of the Chief Information Officer
SSP	System Security Plan
USCCI	United States Cyber Command Instruction
USCCM	United States Cyber Command Manual
USCYBERCOM	United States Cyber Command

Terms

Access control function – Duties involving the process of granting or denying specific requests for obtaining and using information and related information processing services. (CNSSI 4009)

Audit function – Duties involving independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedure. (CNSSI 4009)

Audit log – A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (CNSSI 4009)

Audit record – An individual entry in an audit log related to an audited event. (NIST SP 800-53 Rev 4)

Audit reduction tools – Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (NIST SP 800-12)

Command IS – Information systems under USCYBERCOM configuration control or where USCYBERCOM is responsible for authorizing the system to operate.

Cyberspace Protection Conditions – A uniform system of five progressive readiness conditions (CYBERCON 5, the least restrictive, through CYBERCON 1, the most restrictive) with options for offensive and defensive cyberspace operations. CYBERCONs describe graduated levels of readiness and response options that posture DOD components to secure, operate and defend the DOD Information Network and to deter or defeat adversaries. (CJCSM 6510.01B)

Enclave – A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

Zulu time – Same as Universal Time - A measure of time that conforms, within a close approximation, to the mean diurnal rotation of the Earth and serves as the basis of civil time keeping (JP-05). Zulu time is the time at the prime meridian (Greenwich, England) and is the same everywhere on Earth. It is used by ships, planes and communications as a time standard. Also referred to as Coordinated Universal Time (UTC) which replaced Greenwich Mean Time (GMT).

(<https://www.navy.mil/navydata/questions/zulutime.html> and other internet sources)