BY THE ORDER OF THE COMMANDER
NORTH AMERICAN AEROSPACE
DEFENSE COMMAND (NORAD) AND
UNITED STATES NORTHERN COMMAND
(USNORTHCOM)

NORAD AND USNORTHCOM
INSTRUCTION 10-100

7 FEBRUARY 2013

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: NORAD and USNORTHCOM publications and forms are available on the Headquarters NORAD and USNORTHCOM portal page for downloading at https://portal.noradnorthcom.mil/library/Pubs/SitePages/Home.aspx. All other publications and forms are available at the organizations website.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: N-NC/J39   Certified by: N-NC/CS (MG Charles D. Luckey)

Supersedes NNCI10-100, 5 June 2009   Pages: 8

This instruction implements Department of Defense Directive DODD 5205.02E, ***DOD Operations Security (OPSEC) Program,*** dated 20 June 2012, Department of Defense Manual (DODM), 5205.02-M, ***DOD Operations Security (OPSEC) Program Manual,*** dated 3 November, 2008, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3213.01, ***Joint Operations Security,*** dated 7 May 2012 and Joint Publication (JP) 3-13.3, ***Operations Security,*** dated 4 January 2012. It provides policy guidance and assigns responsibility for the Operations Security (OPSEC) program within North American Aerospace Defense Command (NORAD) and United States Northern Command (USNORTHCOM), components and subordinate Joint Task Forces. This instruction also applies to the Joint Force Maritime Component Commander (JFMCC) when stood up by United States Fleet Forces Command in support of NORAD and USNORTHCOM. This instruction is complementary to the Canadian Forces policy and guidance on OPSEC. It does apply to Air Force Reserve Command (AFRC) units; however, it does not apply to the National Guard units. Send recommendations to change, add, or delete information in this instruction to the Office of Primary Responsibility (OPR) using the AF IMT 847, ***Recommendation for Change of Publication;*** route AF IMT 847s from the field through the appropriate functional's chain of command. See **Attachment 1** for a Glossary of References and Supporting Information. Maintain and dispose of records created as a result of prescribed processes in accordance with the Joint Staff Disposition Schedule CJCSM 5760.01A, ***Joint Staff and Combatant Command Records Management Manual: Vol I (Procedures)*** and ***Vol II (Disposition Schedule).***

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. The following is a list of changes to the superseded version of this instruction. Instructions are simplified and clearly rewritten. NORAD and USNORTHCOM OPSEC program redefined to contain two functions;

planning and administration. Parent Services shall perform administrative functions for subordinate units. OPSEC Planning is performed by OPSEC Planners and integrates OPSEC into all phases of the planning process. Formalized administration functions for HQ NORAD and USNORTHCOM are delegated to the Chief of Staff.

1. **The Need for OPSEC.**

   1.1. Many nations and organizations are actively engaged in collecting information about NORAD and USNORTHCOM. Major sources of information for these groups include the media, the internet and observable activities.

   1.2. The goal of OPSEC is to control unclassified information and observable actions about friendly forces' capabilities, limitations and intentions to prevent or control exploitation by an adversary. To achieve this goal everyone in NORAD and USNORTHCOM must work together to identify which information and observable actions are critical to protect and ensure the success of our operations and take appropriate measures to protect them. Application of the OPSEC Process during all NORAD and USNORTHCOM operations whether in war, crisis or peace and during development of plans and orders will help ensure success in denying information to the adversary.

   1.3. OPSEC is NOT a security function, it is an operations function. Proper use of the OPSEC process will minimize the conflicts between operational and security requirements. The OPSEC process recognizes that risk is inherent in all military activities. The commander or program manager must evaluate each operation and determine the balance between OPSEC measures and operational needs.

2. **NORAD and USNORTHCOM Commanders' OPSEC Objectives.**

   2.1. The NORAD and USNORTHCOM Commander's OPSEC objectives are:

   2.1.1. Make OPSEC a priority within NORAD and USNORTHCOM.

   2.1.2. Integrate OPSEC in all activities and operations that prepare, sustain, or employ NORAD and USNORTHCOM forces during war, crisis or peace.

   2.1.3. Ensure planners recognize the risks associated with compromising critical information and the countermeasures needed to mitigate those risks.

   2.1.4. Continually assess our ability to apply appropriate OPSEC practices in our daily operations.

3. **NORAD and USNORTHCOM OPSEC Program.** To attain the above objectives the NORAD and USNORTHCOM OPSEC program is divided into two functions; OPSEC Planning and OPSEC Administration.

   3.1. OPSEC Planning is performed by OPSEC Planners and integrates OPSEC into all phases of the planning process. The OPSEC Planner shall:

   3.1.1. Participate early in the planning process to provide OPSEC guidance to protect the plan, operation or exercise as well as the planning process.

   3.1.2. Conduct an OPSEC analysis for each phase of the plan, operation or exercise; evaluate each course of action against the commander's acceptable level of risk.

   3.1.3. Develop and promulgate a Critical Information List (CIL) for the plan, operation or exercise.

   3.1.4. Assist in the development and integration of OPSEC countermeasures into the plan,

operation or exercise to reduce vulnerabilities and indicators.

3.1.5.   Develop OPSEC documents to be included in all plans and orders.

3.1.6.   Coordinate the development and integration of OPSEC into information-related capabilities.

3.1.7.   Coordinate with the OPSEC Program Manager (OPM) for surveys or assessments as necessary to identify vulnerabilities during operational planning and execution.

3.1.8.   Coordinate with mission partners to understand and include their OPSEC concerns. Ensure N-NC CIL is understood and protected by mission partners.

3.2.   OPSEC Administration is performed by an OPM and relates to the day-to-day management of the program. The OPM shall:

3.2.1.   Advise the commander, or his delegate, on day-to-day OPSEC matters.

3.2.2.   Develop and maintain the organization's OPSEC program, to include drafting the organization's OPSEC program, policy and guidance documents for the commander's, or his delegate's, approval and signature.

3.2.3.   Identify the organization's critical information; review and update it at least annually or as the organization's mission changes and distribute it within the organization.

3.2.4.   Conduct or coordinate organizational initial and annual OPSEC training for all personnel within the organization.

3.2.5.   Coordinate the conduct of OPSEC assessments and surveys.

3.2.6.   Conduct the organization's annual OPSEC review.

3.2.7.   Develop and maintain an organizational OPSEC continuity binder with applicable documents.

3.2.8.   Establish an OPSEC Working Group (OWG) to promote OPSEC within the organization.

3.2.9.   Coordinate with other security managers, information assurance personnel, knowledge management personnel, anti-terrorism/force protection personnel and critical infrastructure planners to ensure cross-board OPSEC integration and that procedures are in place to control critical information and indicators.

3.2.10. Coordinate with public affairs and others who share the responsibility for the release of information to ensure a rigorous review policy is in place prior to the release of unclassified information.

4. **Responsibilities for OPSEC Planning.**

4.1. Commander NORAD and USNORTHCOM.   Designates NORAD J3 (N/J3) and USNORTHCOM J3 (NC/J3) as having primary responsibility for the NORAD and USNORTHCOM OPSEC planning.

4.2. NORAD/J3 and USNORTHCOM/J3. Designates NORAD and USNORTHCOM/J39 (N-NC/J39) as the command lead OPSEC Planner for NORAD and USNORTHCOM.

4.3. NORAD and USNORTHCOM/J39 (N-NC/J39). N-NC/J39 will:

4.3.1.   Advise the N/J3 and NC/J3 on OPSEC matters that relate to plans, operations and

exercises.

4.3.2. Make recommendations on OPSEC guidance, policy and instructions for NORAD and USNORTHCOM plans, operations and exercises.

4.3.3. Provide assistance to subordinate unit OPSEC Planners and OPSEC program managers as requested.

4.3.4. Appoint a NORAD and USNORTHCOM Lead OPSEC Planner.

4.4. NORAD and USNORTHCOM Lead OPSEC Planner.

4.4.1. The NORAD and USNORTHCOM Lead OPSEC Planner will complete the OPSEC Analysis and Program Management Course (OPSE 2500) or equivalent AND an OPSEC for Planners Course, such as the one offered by 1st Information Operations Command, as soon as practical.

4.4.2. Fulfill the duties identified at **paragraph 3.1.** of this instruction.

4.4.3. Establish and maintain liaison with subordinate element OPSEC Planners to ensure proper execution of OPSEC plans at those levels.

4.4.4. Promulgate OPSEC planning documents applicable to NORAD and USNORTHCOM down to the subordinate elements.

4.4.5. Conduct OPSEC planning and coordination with NORAD and USNORTHCOM battle staff and subordinate staffs for operations, exercises, and activities.

4.4.6. Ensure that the OPSEC Tab to Appendix 3 (Information Operations) to Annex C (Operations) of plans and orders is completed as required. Participate in Joint Planning teams as required.

5. **Responsibilities for OPSEC Administration.**

5.1. Commander NORAD and USNORTHCOM.   The Commander NORAD and USNORTHCOM accepts that subordinate units follow OPSEC direction from parent services for the day-to-day management of OPSEC programs as identified in paragraph 11 of enclosure 2 of DODD 5205.02E and paragraph 4 of Enclosure B of CJCSI 3213.01.

5.2. NORAD and USNORTHCOM Chief of Staff (CS).   Is responsible for the OPSEC Administration function within the Headquarters (HQ) NORAD and USNORTHCOM complex. As a tenant of 21st Space Wing, N-NC HQ will follow the Air Force OPSEC direction for the day-to-day management of its OPSEC program. The CS designates N-NC/J39 as the HQ NORAD and USNORTHCOM OPM. *NOTE: This function does not need to stay within N-NC/J39. DODD 5205.02E states that "OPSEC responsibilities are assigned by commanders and directors to the functional area of their choice."*

5.3. HQ NORAD and USNORTHCOM OPM.

5.3.1. Will complete the OPSEC Analysis and Program Management Course (OPSE 2500) within 90 days.

5.3.2. Fulfill the duties identified at **paragraph 3.2.** of this instruction.

5.3.3. Develop and implement a HQ NORAD and USNORTHCOM OPSEC program to achieve the Commander's OPSEC objectives.

5.3.4. Identify the resources required to ensure the effective implementation of the OPSEC

program.

5.3.5. Establish a HQ NORAD and USNORTHCOM OPSEC training and awareness program.

5.3.6. Monitor the status of OPSEC training for all HQ NORAD and USNORTHCOM personnel.

5.3.7. Provide initial and, as a minimum, annual refresher training for all HQ NORAD and USNORTHCOM personnel.

5.3.8. Provide training as required to the HQ NORAD and USNORTHCOM OPSEC program coordinators.

5.3.9. Coordinate OPSEC support activities for the HQ NORAD and USNORTHCOM OPSEC program coordinators as required.

5.3.10. Coordinate the preparation and publication of the HQ NORAD and USNORTHCOM CIL at least annually, or following any significant changes to the threat or operations.

5.3.11. Conduct HQ NORAD and USNORTHCOM OPSEC assessments annually or as required.

5.3.12. Coordinate and conduct an OPSEC survey at least once every three years. Provide written reports to the Senior Leaders and Commander NORAD and USNORTHCOM.

5.3.13. Complete and staff the HQ NORAD and USNORTHCOM annual OPSEC for submission to the Joint Staff.

5.3.14. Serve as OPR for all OPSEC related matters within HQ NORAD and USNORTHCOM.

5.3.15. Establish and chair a HQ NORAD and USNORTHCOM OWG.

5.3.16. Ensure members of the working group are appointed in writing.

5.3.17. Maintain a HQ NORAD and USNORTHCOM OPSEC continuity folder.

5.3.18. Serve as a member of the 21st Space Wing OWG.

5.4. Directorates and Special Staff.

5.4.1. Appoint an OPSEC coordinator who will promote OPSEC within their organization. Notify the HQ NORAD and USNORTHCOM OPM of any changes to the appointment.

5.4.2. Incorporate OPSEC into all directorate and special staff planning and operations.

5.5. Directorate and Special Staff OPSEC Coordinators.

5.5.1. Serve as members of the HQ NORAD and USNORTHCOM OWG.

5.5.2. Complete as a minimum the OPSEC Fundamentals Course (OPSE 1300) or an approved equivalent within 90 days of appointment. Completion of the OPSEC Program Manager's Course (OPSE 2500) or an approved equivalent is recommended.

5.5.3. Advise their respective organizations on OPSEC issues.

5.5.4. Implement the HQ NORAD and USNORTHCOM OPSEC program within their organization.

5.5.5. Ensure all personnel within their organization can identify their OPSEC coordinator.

5.5.6.   Ensure all personnel within their organization are aware of their OPSEC responsibilities in accordance with this instruction and other instructions as applicable.

5.5.7.   Ensure all personnel within their organization have met the initial and annual OPSEC training requirements.

5.5.8.   Provide input to the HQ NORAD and USNORTHCOM CIL when reviewed.

5.5.9.   Maintain an organization CIL as required.

5.5.10. Support OPSEC surveys and assessments.

5.5.11. Notify the HQ NORAD and USNORTHCOM OPM of any changes to their appointment.

5.6.   The HQ NORAD and USNORTHCOM OWG.

5.6.1.   Meet at least quarterly, or as directed by the Chair.

5.6.2.   Develop and implement HQ NORAD and USNORTHCOM OPSEC program to achieve the Commander's OPSEC objectives.

5.6.3.   Review OPSEC input from directorates and special staffs to develop or revise the N-NC/HQ CIL.

5.7.   NORAD and USNORTHCOM/J2 (N-NC/J2). N-NC/J2 will:

5.7.1.   Obtain, evaluate and provide information on hostile intelligence collection capabilities.

5.7.2.   Provide counter-intelligence and multi-disciplined threat assessments and briefings in support of OPSEC as required.

5.7.3.   Provide advice and assistance regarding physical measures to safeguard critical information concerning HQ NORAD and USNORTHCOM operations and activities.

5.7.4.   Provide advice and assistance concerning intelligence support to OPSEC.

5.8.   NORAD and USNORTHCOM/J6 (N-NC/J6). N-NC/J6 will:

5.8.1.   Communicate any Information Assurance planning and actions which can or should be taken to correct weaknesses and improve the HQ NORAD and USNORTHCOM OPSEC posture.

5.8.2.   Assist in coordinating COMSEC monitoring activities in support of OPSEC objectives.

5.9.   NORAD and USNORTHCOM/PA (N-NC/PA). N-NC/PA will:

5.9.1.   Consider OPSEC before releasing any information to the public.

5.9.2.   Implement a review and approval process for all information posted to official publically accessible web sites.

5.9.3.   Ensure that personnel reviewing official publically accessible web sites have received web OPSEC training.

5.9.4.   Coordinate with region and component public affairs offices to establish an environment where the public's right and need to know is balanced with OPSEC concerns in all public affairs materials available to the media and public.

5.9.5.   Provide specialist assistance with the HQ NORAD and USNORTHCOM OPSEC awareness and training programs.

5.10. HQ NORAD and USNORTHCOM Personnel.

5.10.1. Upon assignment to HQ NORAD and USNORTHCOM complete the initial OPSEC training program.

5.10.2. Complete assigned OPSEC training programs. All liaison officers assigned and working with NORAD and USNORTHCOM will accomplish OPSEC training or provide proof of service specific annual OPSEC training.

5.10.3. Know your OPSEC program coordinator.

5.10.4. Know HQ NORAD and USNORTHCOM Commander's OPSEC objectives.

5.10.5. Know what the critical information is for your environment.

5.10.6. Apply the OPSEC process during planning, operations and daily routines.

5.10.7. Report poor OPSEC practices and divulgence of critical information to your OPSEC coordinator.

5.10.8. Apply the following OPSEC measures:

5.10.8.1. Dispose of all paper waste, except trash items (i.e. newspapers, food wrappers, tissues, etc) in burn bags or shredders.

5.10.8.2. Be aware of who is around you, do not discuss critical information where you can be overheard.

5.10.8.3. Use "Phone Up" or "Open Line" procedures when placing or receiving phone calls within the workspace if there is a possibility of surrounding conversations being picked up by your phone.

ANDRÉ VIENS
Major-General, RCAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DODD 5205.02E, *DOD Operations Security (OPSEC) Program,* June 20, 2012

DODM 5205.02-M, *DOD Operations Security (OPSEC) Program Manual,* 3 November 2008

CJCSI 3213.01, *Joint Operations Security,* 7 May 2012

JP 3-13.3, *Operations Security,* 4 January 2012

AFI 10-701, *Operations Security,* 8 June 2011

Terms

Critical Information List (CIL)—A list of critical information that has been fully coordinated within an organization and approved by the senior decision maker, and is used by all personnel in the organization to identify unclassified information requiring application of OPSEC measures.

Operations Security (OPSEC)—A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to (a) identify those actions that can be observed by adversary intelligence systems, (b) determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Assessment—An evaluative process, usually conducted annually, of an operation, activity, exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence.

OPSEC Process—An analytical process that involves five components: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures

OPSEC Program—A comprehensive process incorporating the principles and practices of OPSEC into an organization.

OPSEC Survey—Conducted at least once every three years, a survey is a collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence processes.