BY THE ORDER OF THE COMMANDER
NORAD/USNORTHCOM

NORAD/USNORTHCOM
INSTRUCTION 33-141

2 OCTOBER 2006
Administrative Change Effective
28 January 2009
Current and Essential, 16 Jul 13

Communications and Information

INFORMATION ASSURANCE/
COMPUTER NETWORK DEFENSE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading on the NORAD - USNORTHCOM Portal (Command Publications and Forms Management) https://operations.noradnorthcom.mil/sites/CommandGroup/ChiefOfStaff/pubsandforms/default.aspx.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: N-NC/Information Assurance

Certified by: CS (Maj Gen John H. Bordelon)
Pages: 7

This instruction implements and expands DODI 8500.2, ***Information Assurance (IA) Implementation*** and CJCSM 6510.01, ***DEFENSE-IN-DEPTH: Information Assurance (IA) and Computer Network Defense (CND)***. DOD and Joint Staff guidance requires DOD components to establish IA and CND policies and assign responsibilities. NORAD and USNORTHCOM (N-NC) considers IA and CND enablers for assured information sharing and are mission critical for command and control systems and as such should be given the utmost priority. For assured information sharing, it is necessary that organizations operating and maintaining NORAD and USNORTHCOM information systems employ IA/CND policies and procedures to satisfy mission objectives and support mission partners' needs. NORAD and USNORTHCOM information exchange processes includes determining what information to share with partners and deploying cross-domain solutions facilitating information sharing based upon Department of Defense (DOD), mission partners and national security requirements. The goals of the NORAD and USNORTHCOM IA/CND program is to provide trusted information systems through the effective employment of the IA/CND elements of NetOps throughout the Commands' information and information systems.

This instruction is applicable to HQ NORAD, HQ USNORTHCOM, NORAD Regions/Sectors, Subordinate Commands, and interagency/non-governmental organizations operating or maintaining NORAD-USNORTHCOM networks and information. It also applies to all NORAD and USNORTHCOM network users.

Nothing in this instruction shall alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations.

Maintain and dispose of records created as a result of prescribed processes in accordance with the Joint Staff Disposition Schedule CJCSM 5760.01 ***Joint Staff and Combatant Command Records Management Manual***: ***Vol I (Procedures) & Vol II (Disposition Schedule)*** which may be found on-line at: http://www.dtic.mil/cjcs_directives/cdata/unlimit/m576001v1.pdf
http://www.dtic.mil/cjcs_directives/cdata/unlimit/m576001v2.pdf

1. Information Assurance and Computer Network Defense. NORAD and USNORTHCOM information and information systems incur higher risks due to mission requirements to share information with our partners, to include non-DOD agencies and non-governmental organizations. NORAD and USNORTHCOM assigned and subordinate elements will use common reporting processes and procedures and implement standardized, interoperable, enterprise-wide security management tools. N-NC/J6 implements defense-in-depth to ensure network survivability and information availability within the NORAD Area of Operations (AOO) and USNORTHCOM Area of Responsibility (AOR). The Network Operations Security Center (NOSC) and Theater NetOps Center-North (TNC-N) will oversee CND actions and report execution to Joint Task Force-Global Network Operations (JTF-GNO).

2. Roles and Responsibilities.

2.1. Designated Approving Authority (DAA) for NORAD and USNORTHCOM information systems will:

2.1.1. Implement IA certification and accreditation (C&A) processes for systems and applications installed on NORAD and USNORTHCOM enterprise networks.

2.1.2. Implement NORAD and USNORTHCOM IA training and certification programs to increase information security awareness.

2.1.3. Manage and assess the effectiveness of the NORAD and USNORTHCOM IA program.

2.1.4. Enforce directives from OSD, DOD, JTF-GNO, and Defense Information Systems Agency (DISA).

2.2. N-NC Enterprise Operations Support will:

2.2.1. Perform system and network configuration management.

2.2.2. Provide 24/7 on-call NORAD and USNORTHCOM enterprise support to include daily operations and exercise support.

2.2.3. Comply with DISA and NORAD and USNORTHCOM information assurance and security requirements.

2.2.4. Implement automated network management functions to perform problem detection, fault correction, fault isolation, diagnosis, and problem tracking until the problem(s) are corrected.

2.2.5. Monitor networks to establish anomaly, fault, and intrusion detection capabilities in accordance with JTF-GNO and local directives.

2.2.6. Implement protective devices to identify and defend against anomalies/attacks/ distribution from external/internal threats and natural causes.

2.2.7. Implement a defensive capability that contains, recovers, restores, and reconstitutes itself against incidents (e.g., failure, misuse, intrusion).

2.2.8. Implement response activities (hardening system/network defenses, containment, recovery, restoration, and reconstitution) to lessen or negate operational consequences of an incident that cause information system/network capability/performance degradation throughout the incident lifecycle (triage, assessment, response, closure).

2.2.9. Employ a role-based enterprise wherein unique user privileges are managed.

2.2.10. Manage identities, attributes, authentication credentials, and authorization of users.

2.2.11. Use the Vulnerability Management System (VMS) to report information assurance status for systems/networks under N-NC/J62 operational control.

2.2.12. Ensure C&A activities are completed during requirement, design, and implementation phases.

2.2.13. Act as Program Manager for NIPRNET, SIPRNET, and RELCAN and assist the N-NC Information Assurance Branch author the DOD Information Assurance Certification and Accreditation Process (DIACAP) package.

2.2.14. Develop Techniques, Tactics, and Procedure (TTP) to monitor NORAD and USNORTHCOM enterprise IA/CND tools and react accordingly.

2.2.15. Participate in NetOps assessment brief.

2.3. N-NC Information Assurance Branch will:

2.3.1. Provide COCOM input to OSD, DOD, JTF-GNO, USSTRATCOM, and Joint Staff policies and doctrine in consultation with N-NC/J39.

2.3.2. Coordinate IA activities with JTF-GNO, National Security Agency, and Combatant Command/Service/Agencies (CC/S/A).

2.3.3. Write, coordinate, and assist in enforcing policies across CC/S/As and AOO/AOR.

2.3.4. Oversee C&A activities for HQ, Regions/Sectors, and Subordinate Commands.

2.3.5. DELETE.

2.3.6. Provide Regions/Sectors and Subordinate Commands with policy guidance.

2.3.7. Appoint and train IA personnel at Regions and Subordinate Commands.

2.3.8. Perform IA staff assistance visits for Regions and Subordinate Commands.

2.3.9. Participate in NetOps Assessment briefings.

2.3.10. Provide network classified material incident support to NOSC.

2.3.11. Ensure all NORAD and USNORTHCOM information systems, C2 systems and networks are certified and accredited.

2.3.12. Ensure NORAD and USNORTHCOM users receive appropriate IA training.

2.3.13. Promote IA/Information Protect with non-DOD mission partners (Canada, Mexico, agencies, first responders, and industry).

2.3.14. Support compliance inspections.

2.3.15. Serve as the primary IA technical advisor to the DAA.

2.3.16. Provide IA/CND exercise support as required.

2.3.17. Serve as the incident response lead and liaison when outside assistance is required.

2.3.18. Manage and conduct IA assessment program.

2.3.19. Conduct annual Federal Information System Management Act (FISMA) reporting.

2.3.20. Conduct Ports, Protocols, and Services (PPS) management.

2.4. N-NC Network Operations Security Center will:

2.4.1. Lead, prioritize, and direct theater Global Information Grid (GIG) assets and resources to ensure they are optimized to support NORAD and USNORTHCOM missions and operations.

2.4.2. Continuously monitor and assess the availability and protective posture of the GIG to support resident CC/S/As missions and operations within the NORAD and USNORTHCOM AOO/AOR.

2.4.3. Implement a network common operational picture to increase shared awareness and understanding across the enterprise.

2.4.4. Implement effective indications and warning of potential or ongoing attacks against the enterprise.

2.4.5. Obtain information on the theater sensor grid to maintain information assurance situational awareness.

2.4.6. Report IA/CND status to JTF-GNO as required.

2.4.7. Analyze, distribute and coordinate responses to Information Assurance Vulnerability Management (IAVM) Alerts, Bulletins and Tech Advisories and Communications Tasking Orders (CTOs).

2.4.8. Track compliance data for Headquarters, Regions/Sectors and Subordinate Commands.

2.4.9. Compile, build and brief the morning NetOps Assessment brief.

2.4.10. Provide 24/7 theater NetOps support as directed in the NetOps CONOPS.

2.4.11. Coordinate NetOps actions with users to minimize disruptions.

2.4.12. Manage Theater INFOCON events and reporting.

2.4.13. Coordinate and prioritize restoral actions.

2.4.14. Assist Regions/Sectors and Subordinate Commands with classified material incident investigations.

2.5. Headquarters, Regions/Sectors, and Subordinate Commands will:

2.5.1. Implement the DOD defense-in-depth strategy that is standardized and interoperable with NORAD and USNORTHCOM enterprise security tools to ensure enterprise situation awareness.

2.5.2. Coordinate with NORAD and USNORTHCOM Information Assurance to deconflict policy issues.

2.5.3. Integrate IA in all network planning and configuration.

2.5.4. Coordinate with NOSC to ensure information exchange requirements are satisfied.

2.5.5. Monitor VMS for IAVM notification and compliance.

2.5.6. Report IAVM status using VMS.

2.5.7. Provide network and/or system DIACAP package to the NORAD and USNORTHCOM Information Assurance Branch for inclusion into the appropriate certification and accreditation products.

2.5.8. Coordinate IA activities with NORAD and USNORTHCOM Information Assurance.

2.6. Interagency and non-governmental organizations will:

2.6.1. Comply with OSD, DOD, USSTRATCOM, DISA, CJCS, and NORAD and USNORTHCOM IA/CND policies and requirements in order to connect to NORAD and USNORTHCOM information systems.

2.6.2. Provide NetOps performance information to the NOSC to support mission requirements.

2.6.3. Identify information exchange requirements necessary for mission support.

2.7. Defense Information Systems Agency Field Security Operations (DISA FSO) will serve as NORAD and USNORTHCOM Tier 2 CND service provider in accordance with the signed Memorandum of Agreement.

2.8. DISA Theater NetOps Center-North will:

2.8.1. Provide to N-NC NOSC IA/CND situational awareness of any potential or ongoing IA/CND attacks against the theater and recommend actions to be taken in response to an ongoing or post-discovery incident.

2.8.2. Provide analysis of incidents. The analysis will be based on similar incidents or activities within the theater and/or across GIG networks to include current attack or malicious code information and experience of the analysts.

2.8.3. Provide defense-in-depth information assurance and promote shared network defense awareness and network understanding across the enterprise. Assist customers in utilization of the IA user-defined picture.

2.8.4. Support assured information sharing by establishing liaisons with JTF-GNO and Canadian Forces Network Operations Support Center.

2.9. 721st Communication Squadron will use the VMS to report IAVM status on NORAD and USNORTHCOM assets under their operational control.

2.10. 153rd Command and Control Squadron will use the VMS to report Information Assurance Vulnerability Alert (IAVA) status on NORAD and USNORTHCOM assets under their operational control.

3. Risk Management. Each NORAD and USNORTHCOM assigned and subordinate element must assess mission, associated risks, and provide the DAA an acceptable risk mitigation analysis. NORAD and USNORTHCOM assigned and subordinate elements will build risk management capabilities, which best balances their security needs, users' needs, and mission requirements. NORAD and USNORTHCOM execute risk mitigation actions through the NOSC utilizing the NetOps operational construct.

4. Certification and Accreditation. In order to assure the availability, integrity, and confidentiality of NORAD and USNORTHCOM information and information systems, NORAD and USNORTHCOM customers and service providers, in coordination with NORAD and USNORTHCOM Information

Assurance Branch, will ensure information systems and networks have completed the DIACAP package and have NORAD and USNORTHCOM DAA approval prior to operations.

J. M. HAMBY, RDML, USN
Director, Command Control Systems

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

NSTISSP No. 11, ***National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products***

DOD Instruction 5200.40***, DOD Information Technology Security Certification and Accreditation Process (DITSCAP)***

CJCSM 6510.01E, ***Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)***

CJCSI 6510.01E, ***Information Assurance (IA) and Computer Network Defense (CND)***

DOD Directive 8500.1E, ***Information Assurance (IA)***

DOD Instruction 8500.2, ***Information Assurance (IA) Implementation***

DOD Directive O-8530.1, ***Computer Network Defense (CND)***

DOD Directive 8570.1, ***Information Assurance (IA) Training, Certification, and Workforce Management***

DOD Net-Centric Information Assurance Strategy