

~~SECRET~~

①



Department of Defense DIRECTIVE

NUMBER S-5210.81

August 8, 2005

Incorporating Change 1, September 11, 2015

USD(AT&L)

SUBJECT: United States Nuclear Weapons Command and Control, Safety, and Security (U)

- References:
- (a) DoD Directive S-5210.81, United States Nuclear Weapons Command and Control (U), June 18, 1991 (hereby cancelled)
 - (b) National Security Presidential Directive-28¹, United States Nuclear Weapons Command and Control, Safety, and Security (U), June 20, 2003
 - (c) Nuclear Posture Review Report² (U), December 2001
 - (d) OMB Circular A-130, Management of Federal Information Resources, Transmittal 4, November 30, 2000
 - (e) through (am), see enclosure 1

1. (U) REISSUANCE AND PURPOSE

1.1. (U) This Directive reissues reference (a) to provide general policy and assignment of responsibilities governing United States nuclear weapons Command and Control (C2), safety, and security within the Department of Defense, as directed by reference (b).

2. (U) APPLICABILITY AND SCOPE. This Directive:

¹ The Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD(AT&L)) is the DoD release authority for this document. All requests for copies shall be made through the OUSD(AT&L), who, in turn, shall request a copy from the National Security Council staff.

² The Office of the Under Secretary of Defense for Policy (OUSD(P)) is the DoD release authority for this document. All requests for copies shall be made through the OUSD(P).

~~SECRET~~

Classified by: ~~Ken Krieg USD(AT&L)~~

Reason: ~~1.5 (a) (f) (g)~~

Declassify on: ~~07/16/2015~~

~~Classified By: Frank Kendall, USD(AT&L)~~

~~Reason: 1.4 (a) (f) (g)~~

~~Declassify On: 20400808~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

2.1. (U) Applies to the Office of the Secretary of Defense (OSD), the Military Services, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components"). The term "Military Services" as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. (U) Provides overarching policy guidance and direction related to nuclear command and control (NC2), safety, and security, and identifies aspects of the Nuclear Command and Control System (NCCS) for which the Department of Defense has individual, or shared, responsibility (including U.S. nuclear weapons systems deployed in support of allied forces under Programs of Cooperation).

2.3. (U) Provides guidance for ensuring the NCCS supports the New Triad through the integration of nuclear and non-nuclear offensive missions and defenses in accordance with reference (b) and the defense strategy framework defined in the Nuclear Posture Review Report (reference (c)).

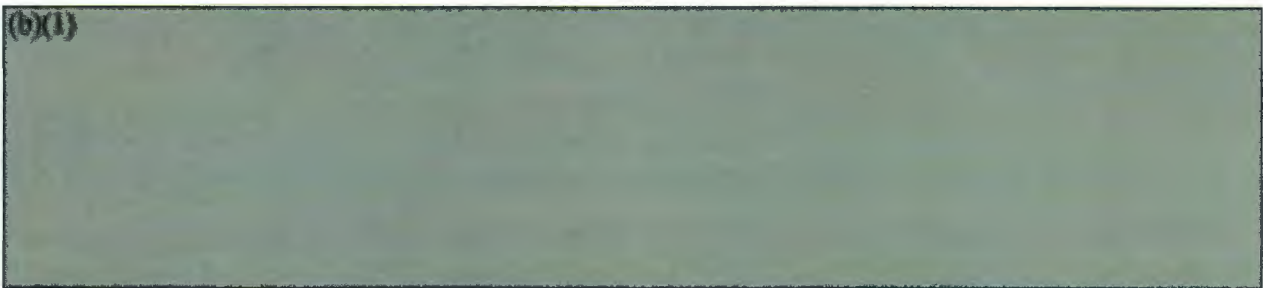
2.4. (U) Describes responsibilities for coordinating NCCS-related activities of DoD Components with other Government Departments and Agencies.

3. (U) DEFINITIONS

3.1. (U) Terms used in this Directive are defined in enclosure 2.

4. (U) POLICY

4.1 (U) It is national policy³ that:



³ General guidance extracted from reference (b).

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

4.1.2. (U) The Department of Defense shall achieve a credible deterrent strategy with the lowest possible number of deployed nuclear weapons consistent with our current and future security requirements and those of our allies. The Department has developed a strategic framework (reference c), which calls for the creation of a New Triad consisting of a mix of nuclear and non-nuclear strike forces, active and passive defenses, and a responsive infrastructure that shall be enhanced by an integrated, collaborative, and adaptive approach to intelligence, C2, and planning.

(b)(1)



4.2. (U) It is DoD policy that:

(b)(1)



4.2.4. (U) As a minimum, DoD NCCS procedures shall meet the Policy criteria contained in enclosure 3.

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

(b)(1)



4.2.5.1. (U) The essential DoD NCCS functions are:

4.2.5.1.1. (U) Situation Monitoring (including Integrated Tactical Warning/Attack Assessment;

4.2.5.1.2. (U) Decision Making;

4.2.5.1.3. (U) Force Direction;

4.2.5.1.4. (U) Force Management; and

4.2.5.1.5. (U) Planning.

(b)(1)



~~SECRET~~

(b)(1)



~~SECRET~~

DoDD S-5210.8L August 8, 2005

(b)(1)



5. (U) RESPONSIBILITIES

5.1. (U) The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) shall, consistent with OSD Memorandum, "United States Nuclear Command and Control, Safety, and Security/NSPD-28" (reference (g)), Deputy Secretary of Defense Memorandum, "Realignment of Responsibilities for Nuclear Weapon Physical Security from the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Acquisition, Technology, and Logistics" (reference (h)), DoD Directive 5134.1 (reference (i)), DoD Directive 5134.8 (reference (G)), and Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence-and Related Matters" (reference (k)), support nuclear weapons C2, safety, and security in the following areas:

5.1.1. (U) Serve as the OSD Principal Staff Assistant (PSA) for coordinating implementation of reference (b) and other policy guidance developed under this Directive, and for advising the Secretary of Defense on implementation of NCCS requirements within the Department of Defense.

5.1.2. (U) Represent the Department of Defense as a member of the NCCS Committee of Principals, in accordance with reference (b).

5.1.3. (U) Establish a two-tier management and oversight structure to assist the Secretary of Defense in executing responsibilities assigned to the Department of Defense under reference (b). The structure shall consist of a four-star/flag-level committee, supported by a two-star/flag-level committee, with membership as indicated in paragraphs 5.1.3.2 and 5.1.3.3. This structure shall review and resolve issues consistent with, and to complement, departmental staffing procedures.

5.1.3.1. (U) The general responsibilities of the committees at each level, related to DoD NC2, safety, and security matters, include:

5.1.3.1.1. (U) Coordinating the implementation of requirements;

5.1.3.1.2. (U) Ensuring a unified and integrated management of DoD assets;

5.1.3.1.3. (U) Identifying programs and capabilities for priority support;

5.1.3.1.4. (U) Ensuring mechanisms are in place to measure mission performance, identify vulnerabilities, and monitor actions to correct deficiencies;

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.1.3.1.5. (U) Ensuring best practices are identified and shared, as appropriate, throughout the Department of Defense;

5.1.3.1.6. (U) Reviewing, as necessary, DoD policies, programs, operations, and equipment that support this Directive;

5.1.3.1.7. (U) Reporting key issues to the Secretary of Defense on an annual basis, in time to affect funding prioritization in the Planning, Programming, Budgeting, and Execution process, and other related policy and planning documents;

5.1.3.1.8. (U) Developing, as appropriate, and reviewing all DoD positions and presentations for the interagency Committee of Principals (CoP).

5.1.3.2. (U) The Senior NSPD-28 Oversight Committee (SNOC) shall be chaired by the USD(AT&L) to advise the Secretary of Defense on implementation of reference (b), and serve in his role as the DoD member of the CoP. The SNOC shall include the following members:

5.1.3.2.1. (U) The Under Secretary of Defense for Policy (USD(P))

5.1.3.2.2. (U) The Vice Chairman of the Joint Chiefs of Staff

5.1.3.2.3. (U) The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD(NII)/DoD CIO)

5.1.3.2.4. (U) Other U.S. Government officials, as determined appropriate by the Committee Chair.

5.1.3.3. (U) The NSPD-28 Oversight Committee (NOC) shall be chaired by the Assistant to the Secretary of Defense (Nuclear and Chemical and Biological Defense Programs) (ATSD(NCB)) and vice-chaired by the Deputy Assistant Secretary of Defense (C3 Policies & Programs & Space Programs). The NOC shall include member/observer representatives from the following organizations:

5.1.3.3.1. (U) A representative of each Military Service, as designated by the Secretaries of the Military Services (Member)

5.1.3.3.2. (U) The Office of the USD(P) (Member)

5.1.3.3.3. (U) The Office of the Under Secretary of Defense for Intelligence (USD(I)) (Member)

5.1.3.3.4. (U) The Office of the Under Secretary of Defense Comptroller/Chief

~~SECRET~~

Change 1, 09/11/2015

~~SECRET~~

DoDD S-5210.81, August 8, 2005

Financial Officer (USD(C/CFO)) (Observer)

5.1.3.3.5. (U) United States Strategic Command (USSTRATCOM) (Member)

5.1.3.3.6. (U) The Office of the Director, Program Analysis and Evaluation
(Observer)

5.1.3.3.7. (U) The Defense Information Systems Agency (DISA) (Observer)

5.1.3.3.8. (U) The Defense Threat Reduction Agency (Observer)

5.1.3.3.9. (U) The National Security Agency (NSA) (Observer)

5.1.3.3.10. (U) Representatives from the Joint Staff J3, J5, and J6 Directorates, as
designated by their Directors (Member)

5.1.3.3.11 (U) Other U.S. Government officials, as determined appropriate by the
committee chair/vice chair.

(b)(3):10 USC §128

5.1.5. (U) Develop integrated policy and standards for nuclear weapons system safety, security, and weapons-level use control, and establish survivability and reliability criteria and standards for related nuclear weapons delivery systems and equipment, in coordination with the Secretaries of the Military Services, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), the ASD(NII)/DoD CIO, and the Directors of the appropriate Defense Agencies.

5.1.6. (U) In collaboration with the Department of Energy, and in coordination with the Military Services, develop and implement directives, instructions, and procedures, and acquire capabilities to safely and securely store and move nuclear weapons.

5.1.7. (U) Coordinate the development of agreements between the Department of Defense, the Department of Energy, and other U.S. Government Departments and Agencies relative to technology, acquisition, modification, security, and safety for nuclear weapons and applicable NCCS components.

(b)(1)

~~SECRET~~

Change 1, 09/11/2015

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.1.9. (U) Develop policy and procedures to ensure that identified critical equipment is survivable prior to design. Ensure survivability of such equipment is recognized as a major factor during development and acquisition.

5.1.10. (U) In collaboration with the Department of Energy, serve as the primary office of responsibility within the Department of Defense for development of an annual Joint Surety Report to the President that assesses, as a minimum, nuclear weapon safety, security, control, emergency response, inspection, and evaluation programs, and the impact of budget constraints on required improvement programs.

5.1.11. (U) In coordination with the USD(P), the USD(C/CFO), the USD(I), and the ASD(NII)/DoD CIO, review and evaluate DoD Component plans, programs, and budget submissions for adherence to established priorities, policies and procedures, standards, and resource guidance to support this Directive and ensure the development of resources to support plans, procedures, and capabilities to recover lost, missing, or stolen nuclear weapons or nuclear components.

(b)(1)



5.1.13. (U) In coordination with the Military Services, the Chairman of the Joint Chiefs of Staff, and the USD(P), and in collaboration with other U.S. Government Departments and Agencies, develop policies, procedures, and standards, and regularly exercise plans for response to nuclear accidents and incidents (inside and outside the United States or its territories) involving nuclear weapons or components in DoD custody.

5.1.14. (U) In coordination with the Chairman of the Joint Chiefs of Staff, the USD(P), the ASD(NII)/DoD CIO, and in collaboration with other U.S. Government Departments and Agencies, evaluate threat assessments and develop security policies, procedures, and standards to identify and protect nuclear weapons, nuclear components, and critical NCCS facilities and equipment from loss, theft, sabotage, and accidental damage or destruction.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.1.16. (U) Ensure the Military Services conduct vulnerability analyses, realistic training and evaluations, and force-on-force exercises, for NCCS security elements, against existing and emerging threats at all levels using performance-based standards, where possible.

5.1.17. (U) In collaboration with the Department of Energy, and in coordination with the Military Services and other U.S. Government Departments and Agencies, conduct research and development to identify and employ new technologies to deny unauthorized access to nuclear weapons and critical NCCS equipment and facilities and improve overall security.

(b)(1)



5.2. (U) The Director, Defense Threat Reduction Agency, under the USD(AT&L), shall assist other appropriate organizations to ensure that balanced survivability assessments are conducted for NCCS assets.

5.3. (U) The Under Secretary of Defense for Policy shall, consistent with DoD Directive 5111.1 (reference (m)), support NC2, safety, and security in the following areas:

5.3.1. (U) In coordination with the Chairman of the Joint Chiefs of Staff, the USD(AT&L), and the ASD(NII)/DoD CIO, develop policy and establish standards to identify and protect critical NCCS technologies against inadvertent transfer to foreign states or non-state entities.

5.3.2. (U) In coordination with the Chairman of the Joint Chiefs of Staff and the USD(AT&L), develop mission assurance policies for the exercise, training, and augmentation of personnel to ensure that NCCS capabilities are maintained at the appropriate degree of readiness and can support the NCCS decision-making process under all conditions.

5.3.3. (U) In coordination with the Chairman of the Joint Chiefs of Staff and the USD(AT&L), provide oversight of endurability requirements for NCCS facilities and equipment.

5.3.4. (U) In coordination with the Chairman of the Joint Chiefs of Staff, the USD(AT&L), and the Combatant Commanders, ensure NCCS capabilities and requirements are appropriately considered in developing DoD positions on U.S. arms control negotiations.

5.3.5. (U) In coordination with the USD(AT&L) and the USD(I), implement NCCS Procedures and Policy Guidance contained in enclosures 3 through 6.

5.4. (U) The Under Secretary of Defense for Intelligence shall, consistent with Deputy Secretary of Defense guidance in references (h) and (k), support NC2, safety, and security in the following areas:

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

(b)(1)



5.4.3. (U) Establish and oversee the implementation of policies and procedures for the conduct of the DoD Operational Security (OPSEC) Program including monitoring, evaluating, and periodically reviewing all DoD OPSEC activities.

(b)(1)



5.4.5. (U) In coordination with the USD(AT&L) and the USD(P), implement NCCS Procedures and Policy Guidance contained in enclosures 3 through 6.

5.5. (U) The Director, National Security Agency, under the USD(I), as the National Manager for National Security Telecommunications and Information Systems Security, consistent with National Security Directive 42 (reference (n)), shall act as the focal point for cryptography, telecommunications system security, and information systems security for national security systems. NSA shall assist the Chairman of the Joint Chiefs of Staff, the USD(AT&L), and the ASD(NII)/DoD CIO in developing NC2 standards and evaluating NCCS program performance.

5.6. (U) The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer shall support NC2, safety, and security in the following areas, consistent with DoD Directive 5144.1 (reference (o)):

5.6.1. (U) Serve as the OSD PSA for coordinating the development of Command, Control, and Communications (C3) policy and providing OSD staff oversight of C3 programs that support the NCCS.

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.6.2. (U) Ensure coordination of DoD NCCS activities with other U.S. Government Departments and Agencies as appropriate, except those assigned elsewhere in this Directive.

5.6.3. (U) In collaboration with the Military Services, the Chairman of the Joint Chiefs of Staff, the USD(AT&L), the USD(P), the USD(C/CFO), and the USD(I), develop additional implementation guidance and review DoD programs to ensure compliance with the communications policies described in enclosures 3 through 6 and to achieve other C2 objectives identified in this Directive.

5.6.4. (U) Designate a Deputy Assistant Secretary of Defense to serve as the Vice Chairman of NOC. (See subparagraph 5.1.3.3.)

(b)(1)



5.6.7. (U) In coordination with the Chairman of the Joint Chiefs of Staff, the USD(AT&L), the USD(P), the USD(I), and the Commander, USSTRATCOM, evaluate the NCCS to ensure the appropriate level of support for the New Triad, as approved by the President and the Secretary of Defense.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

(b)(1)



5.6.10. (U) Establish and oversee the implementation of policies and procedures for the conduct of the DoD Information Assurance Program including monitoring, evaluating, and periodically reviewing all DoD Information Assurance activities.

5.7. (U) The Director, Defense Information Systems Agency, under the ASD(NII)/DoD CIO as the Nuclear C3 Technical Systems Engineer, shall assist the Chairman of the Joint Chiefs of Staff, the USD(AT&L), and the ASD(NII)/DoD CIO, in developing NC2 standards and evaluating NCCS program performance.

5.8. (U) The Directors of the Defense Agencies shall:

5.8.1. (U) Provide appropriate technical, engineering evaluation, and selected systems management assistance on a continuing basis in support of the NCCS, as tasked.

5.8.2. (U) Ensure the standards and guidance promulgated as a result of this Directive are incorporated in the NCCS structure over which the agency has designated responsibilities.

5.8.3. (U) Maintain communications security and information assurance programs to ensure operations are not compromised. This responsibility includes maintaining control of wireless access to information systems to ensure the wireless systems (including external interfaces to commercial wireless services) do not introduce wireless vulnerabilities that undermine the assurance of the other interconnected systems.

5.9. (U) The Secretaries of the Military Services shall:

5.9.1. (U) Ensure that designated critical NCCS elements, under the cognizance of their respective Military Services, are trained, exercised, and maintained at the established degrees of readiness and generation, and that these elements also meet the established nuclear training, survivability, reliability, and endurance standards.

5.9.2. (U) Implement use control standards and develop and employ positive measures for security, safety, control, and protection against physical damage, misuse, and theft of nuclear weapons, nuclear components, and NCCS components and facilities for which the Military Department has responsibility.

5.9.3. (U) Provide for internal and external inspections, vulnerability analyses, realistic training and evaluations, and force-on-force exercises against existing and emerging threats at all

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

levels using performance-based standards, where possible. These actions, together with other capabilities measurements (e.g., personnel, logistics), should be integrated to provide a balanced evaluation of readiness and to ensure design capabilities meet established performance standards. The results of these inspections and analyses shall be reported to the Chairman of the Joint Chiefs of Staff through established readiness reporting channels.

5.9.4. (U) Develop plans, procedures, and capabilities, and provide resources to work with other organizations to recover lost or stolen nuclear weapons or nuclear components.

5.9.5. (U) Ensure that designated individuals assigned to NCCS positions are subject to personnel reliability measures promulgated by this Directive and other follow-on guidance.

5.9.6. (U) Ensure that standards and requirements promulgated by this Directive, and other follow-on guidance, are included, as appropriate, into the organizational inspection programs.

5.9.7. (U) Provide operational security guidance for assigned NCCS communications and automated information systems.

5.9.8. (U) Maintain communications security and information assurance programs to ensure operations are not compromised. This responsibility includes maintaining control of wireless access to information systems to ensure the wireless systems (including external interfaces to commercial wireless services) do not introduce wireless vulnerabilities that undermine the assurance of the other interconnected systems.

5.9.9. (U) Ensure resources are provided for assigned NCCS systems to meet the programming, planning, and budget requirements contained in enclosures 3 through 6.

5.9.10. (U) Establish, fund, and maintain throughout their lifecycle, nuclear hardness maintenance/hardness surveillance programs for those NCCS assets designated and designed to operate through, or otherwise survive, nuclear effects.

5.9.11. (U) Place the highest logistic support priority to the Chairman of the Joint Chiefs of Staff-designated NCCS critical equipment.

5.10. (U) The Chairman of the Joint Chiefs of Staff, consistent with Section 153, Title 10 of United States Code (reference (u)), shall support NC2, safety, and security in the following areas:

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

(b)(1)



5.10.4. (U) Develop a means to identify, prioritize, and monitor critical NCCS systems (to include NC2 equipment and facilities) to ensure actions are taken to meet nuclear survivability requirements, reliability criteria, security, and endurance standards specified in this and other supporting issuances.

5.10.5. (U) Identify, review, and support in the annual budget process, as necessary, critical NCCS systems, equipment, facilities, and supporting elements required to meet the policy guidance of this Directive, and provide the critical capabilities to support the full range of military operations under the New Triad concept.

5.10.6. (U) Prepare an annual list of prioritized NCCS critical equipment and facilities, and provide the list to the ASD(NII)/DoD CIO and the ATSD(NCB).

5.10.7. (U) Ensure the viability of critical NCCS assets through the following actions:

(b)(1)



5.10.7.2. (U) Establish the mandatory KPPs for endurability and survivability (including EMP hardening). This process shall be conducted through the Joint Requirements Oversight Council, in coordination with the USD(AT&L), the USD(P), and the ASD(NII)/DoD CIO. Any decision to lessen NCCS critical asset survivability and endurability must be approved by the USD(AT&L) or the ASD(NII)/DoD CIO for Major Defense Acquisition Programs (MDAP) and by Military Service Acquisition Executives for non-MDAP acquisitions.

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.10.8. (U) In coordination with the Military Services and the Combatant Commanders, identify specific groupings of, or individual, personnel billets associated with nuclear weapons C2, security, safety, and maintenance that shall be subject to personnel reliability standards. As the New Triad C2 structure evolves, including the NCCS, identify any additional groupings of personnel that should be subject to personnel reliability standards.

5.10.9. (U) Establish nuclear weapons technical inspection policy and monitor implementation of the inspection system.

5.10.10. (U) Develop and maintain NCCS plans and procedures:

5.10.10.1. (U) In coordination with the USD(AT&L), the USD(P), and the USD(I), to implement NCCS Procedures and Policy Guidance contained in enclosures 3 through 6.

5.10.10.2. (U) To implement the full range of the U.S. nuclear weapons employment policy.

(b)(1)



5.10.10.5. (U) Where operational or security considerations restrict the use of NCCS equipment for training/exercise, develop a capability to simulate that equipment as realistically as possible.

5.10.10.6. (U) Assist in the recovery of lost, missing, or stolen nuclear weapons or nuclear components.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.10.10.10. (U) In coordination with the ASD(NII)/DoD CIO, develop the technical performance standards for the DoD elements of the NCCS and ensure they support and complement future technical performance guidance developed by the Joint Staff relating to the expanded C2 structure for the evolving New Triad.

5.10.10.11. (U) Ensure that standards and requirements promulgated by this Directive, and other follow-on guidance, are included, as appropriate, in the organizational inspection programs.

5.11. (U) The Commanders of the Combatant Commands⁴ through the Chairman of the Joint Chiefs of Staff, shall develop, implement, and maintain NCCS plans and procedures to:

5.11.1. (U) Support the full applicable range of U.S. nuclear weapons employment policy.

5.11.2. (U) Ensure that NCCS elements under their control are maintained at an appropriate degree of readiness and generation.

5.11.3. (U) Ensure adherence to standards for nuclear weapon safety, security, and control.

5.11.4. (U) Ensure control of nuclear weapons and/or components, applicable weapons systems, and operational NCCS code and/or authentication systems under their purview.

5.11.5. (U) Ensure physical security and protection against physical damage, misuse, and theft of all nuclear weapons and nuclear components under their control.

(b)(1)

5.11.7. (U) Establish plans and procedures to relocate operationally deployed nuclear weapons to any specified location to ensure their security and availability for use in response to changes in operational requirements, natural disaster, or crisis situations.

(b)(1)

⁴ Detailed NC2 responsibilities for selected Combatant Commanders are further delineated in "The Unified Command Plan" (reference (v)).

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

5.11.9. (U) Assist in the development of plans, procedures, and capabilities, and provide resources to work with other organizations to recover lost, stolen, or missing nuclear weapons or nuclear components.

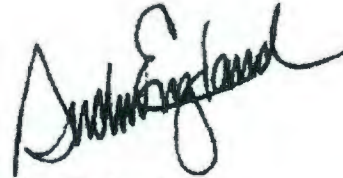
5.11.10. (U) Ensure that standards and requirements promulgated by this Directive, and other follow-on guidance, are included, as appropriate, in the organizational inspection programs.

5.11.11. (U) Maintain a Personnel Reliability Program, in compliance with DoD Directive 5210.42 (references (w)) and DoD 5210.42-R (reference (x)), that establishes procedures, responsibilities, and capabilities to monitor all personnel associated with the NCCS program.

5.11.12. (U) In coordination with the USD(AT&L), the USD(P), and the USD(I), implement NCCS Procedures and Policy Guidance contained in enclosures 3 through 6.

6. (U) EFFECTIVE DATE

(U) This Directive is effective immediately.



Gordon England
Acting Deputy Secretary of Defense

Enclosures - 6

- E1. References, continued
- E2. Definitions
- E3. Additional Policy Regarding NCCS Procedures
- E4. Additional Policy Regarding Critical NCCS Equipment and Facilities
- E5. Additional Policy Regarding NCCS Communications
- E6. Additional Policy Regarding Safety, Security, and Control of Nuclear Weapons

~~SECRET~~

UNCLASSIFIED

DoDD S-5210.81, August 8, 2005

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
- (f) DoD Directive 8500.1, "Information Assurance," October 24, 2002
- (g) Office of the Secretary of Defense Memorandum, "United States Nuclear Command and Control, Safety, and Security/NSPD-28," July 19, 2004
- (h) Deputy Secretary of Defense Memorandum, "Realignment of Responsibilities for Nuclear Weapon Physical Security from the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Acquisition, Technology, & Logistics," July 19, 2004
- (i) DoD Directive 5134.1, "Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))," April 21, 2000
- (j) DoD Directive 5134.8, "Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB))," June 8, 1994
- (k) Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence - and Related Matters," May 8, 2003
- (l) DoD S-5210.41-M, "Nuclear Weapon Security Manual (U)," November 22, 2004
- (m) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
- (n) National Security Directive 42⁵, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
- (o) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII/DoD CIO))," May 2, 2005
- (p) DoD Directive 4640.6, "Communications Security, Telephone Monitoring and Recording," June 26, 1981
- (q) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
- (r) DoD Directive 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004
- (s) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (t) Section 2224, Title 10 of United States Code
- (u) Section 153, Title 10 of United States Code
- (v) "The Unified Command Plan 2002⁶ (U)," March 1, 2005
- (w) DoD Directive 5210.42, "Nuclear Weapons Personnel Reliability Program (PRP)," January 8, 2001

⁵ The Office of the Assistant Secretary of Defense (Networks and Information Integration) is the DoD release authority for this document. All requests for copies shall be made through the OASD(NII), who, in turn, shall request a copy from the National Security Council staff.

⁶ The Chairman of the Joint Chiefs of Staff is the DoD release authority for this document. All requests for copies shall be made through the Joint Staff (Comment: This document is available on the JS website to anyone with SIPRNET access)

UNCLASSIFIED

UNCLASSIFIED

DoDD S-5210.81, August 8, 2005

- (x) DoD 5210.42-R, "Department of Defense Nuclear Weapon Personnel Reliability Program (PRP) Regulation," January 8, 2001
- (y) Section 2315, Title 10 of United States Code
- (z) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
- (aa) DoD Directive O-5210.41, "Security Policy for Protecting Nuclear Weapons," November 1, 2004
- (ab) DoD Instruction C-5210.82, "Protection of Nuclear Weapons Coding Equipment (U)," July 2, 1991
- (ac) DoD Directive 3150.3, "Nuclear Force Security and Survivability (S2)," August 16, 1994
- (ad) DoD Directive 3150.2, "DoD Nuclear Weapon System Safety Program," December 23, 1996
- (ae) DoD 3150.2-M, "DoD Nuclear Weapon System Safety Program Manual," December 23, 1996
- (af) DoD Directive S-3150.7, "Controlling the Use of Nuclear Weapons (U)," June 20, 1994
- (ag) DoD Directive 3150.8, "DoD Response to Radiological Accidents," June 13, 1996
- (ah) DoD 3150.8-M, "Nuclear Weapon Accident Response Procedures (NARP)," February 22, 2005
- (ai) DoD Directive 4540.5, "Logistic Transportation of Nuclear Weapons," February 4, 1998
- (aj) DoD 4540.5-M, "DoD Nuclear Weapons Transportation Manual," February, 1998
- (ak) DoD Directive 3150.5, "DoD Response to Improvised Nuclear Device (IND) Incidents," March 24, 1987
- (al) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978
- (am) DoD Directive S-5200.16, "Objectives and Minimum Standards for Communications Security Measures Used in Nuclear Command and Control Communications (U)," September 22, 1970

UNCLASSIFIED

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E2. ENCLOSURE 2

DEFINITIONS

E2. (U) For purposes of this directive, the following definitions apply:

E2.1. (U) Assured. The capability to operate with certainty.

(b)(1)



E2.3. (U) Command and Control (C2). The exercise of authority and direction, by a properly designated commander, over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in accomplishment of the mission

E2.4. (U) Continuous. The capability of uninterrupted conduct of functions, tasks, or duties necessary to accomplish a military action or mission.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

(b)(1)

E2.7. (U) Designated Nuclear Command and Control Personnel. These include, but are not necessarily limited to, those personnel with access to the NCCS coding and authentication processes and a communications medium necessary to transmit release, execution, or termination orders; those personnel involved in the preparation and production of NCCS coding and authentication documents and equipment, those personnel involved in preparation and production of nuclear weapons targeting tapes and materials; or those maintenance and security personnel who could have an adverse effect on system performance for nodes and equipment that represent near-single-point-failure elements for the NCCS.

E2.8 (U) Endurability. The property of a system, subsystem, equipment, or process that enables it to continue to function within specified performance limits for an extended period of time, usually months, despite a severe natural or man-made disturbance, such as a nuclear attack, or a loss of external logistic or utility support. Endurability is not compromised by temporary failures when the local capability exists to restore and maintain the system, subsystem, equipment, or process to an acceptable performance level.

E2.9. (U) Enduring. The capability to sustain operations at specified levels of performance before, during, and after hostile events or operating within stressed environments.

E2.10. (U) Flexible. The capability of meeting changing situations with timely, effective, appropriate, and adaptable reaction to the full range of plausible scenarios.

E2.11. (U) Firmware. Involves programming functions implemented through a small special-purpose memory unit.

E2.12. (U) Global Information Grid (GIG). The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand for war-fighters, policy makers, and support personnel.

E2.13. (U) Information Assurance. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.14. (U) National Military Command System (NMCS). Designed to support the President and the Secretary of Defense in exercising their responsibilities for crisis response and for the direction of U.S. Armed Forces, and the Chairman of the Joint Chiefs of Staff in

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

executing his responsibilities. The NMCS consists of facilities including the National Military Command Center, and other fixed/mobile command centers designated by the Secretary of Defense. The NMCS also includes supporting data processing systems and networks, display systems, communications systems, procedures, and personnel.

E2.15. (U) Telecommunications and Information Systems Security. The protection afforded to telecommunications and information systems to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptographic security, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary. This function also applies to the physical protection of technical security material and technical security information (definition derived from reference (n)).

E2.16. (U) National Security Systems. Those telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in Section 2315, Title 10 of United States Code (reference (y)), that involve C2 of military forces, involve equipment that is an integral part of a weapon or weapon system, or involve equipment that is critical to the direct fulfillment of military or intelligence missions.

E2.17. (U) Nuclear Command and Control (NC2). The exercise of authority and direction by the President, as Commander in Chief of U.S. Armed Forces, through established command lines, over nuclear weapon operations of military forces; as Chief Executive over all Government activities that support those operations; and as Head of State over required multinational actions that support those operations. The NC2 structure supports the exercise of authority and direction by the President.

(b)(1)



E2.18.2. (U) Provide the means to ensure the use of U.S. nuclear weapons and warheads, when authorized, and to prevent unauthorized or accidental use;

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E2.18.3. (U) Protect critical information and information systems; and,

E2.18.4. (U) Maintain a supporting infrastructure that assures the reliability of current capabilities and can respond to future requirements.

E2.19. (U) Positive Measures. The combination of procedural and administrative actions, physical safeguards, and design features expressly for the purpose of ensuring security, safety, and control of nuclear weapons and systems, including associated personnel.

E2.20. (U) Reliable. The capability of performing its intended function at required levels, for a specified interval, under stated conditions.

E2.21. (U) Responsive. The capability to react within a specified period to accomplish a designated objective.

E2.22. (U) Robust. The qualitative measure of a system, capability, or process to withstand across a range of plausible events or stressed environments, or recover gracefully to specified levels. This measure is primarily influenced by two factors: ruggedness and redundancy.

E2.23. (U) Secure. The capability to ensure a state of protection against hostile or unauthorized acts, influences, or disclosure.

E2.24. (U) Survivable. The capability to avoid or withstand hostile and/or stressed environments. For DoD NCCS elements identified as critical, this capability shall be obtained through a combination of systems that can both "operate through" and/or "recover from" the most hostile threat environments to ensure the uninterrupted control of nuclear weapons.

(b)(1)

E2.26. (U) Unbroken. See Continuous.

(b)(1)

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E3. ENCLOSURE 3 (U)

ADDITIONAL POLICY REGARDING NCCS PROCEDURES (U)

E3.1. (U) NCCS procedures shall, at a minimum:

(b)(1)



E3.1.5. (U) Ensure adherence to standards for nuclear weapon safety, security, and control.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

(b)(1)



E3.1.10. (U) Provide for internal and external inspections, vulnerability analyses, realistic training and evaluations, and force-on-force exercises against existing and emerging threats at all levels using performance-based standards, where possible. These actions, together with other capabilities measurements (e.g., personnel, logistics), should be integrated to provide a balanced evaluation of readiness and to ensure design capabilities meet established performance standards.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E4. ENCLOSURE 4 (U)

ADDITIONAL POLICY REGARDING CRITICAL NCCS EQUIPMENT
AND FACILITIES (U)

E4.1. (U) Critical NCCS equipment is that equipment required to achieve national policy objectives for the readiness, security, and execution of nuclear weapons through all environments. Critical equipment and facilities shall be identified to meet the general policy guidance of this directive regarding nuclear survivability and endurability. (See paragraph 4.) Critical equipment shall be designated annually in writing by the Chairman of the Joint Chiefs of Staff in accordance with paragraph 5.10.4., and the list shall be provided to the ASD(NII)/DoD CIO. DoD NCCS organizations shall review their assigned critical equipment annually and submit a status of their reviews and recommendations related to the critical equipment lists to the Chairman of the Joint Chiefs of Staff by September 30 of each year. Additionally, the following specific policies apply:

(b)(1)



E4.1.3. (U) Training and exercises should normally involve the use of fielded equipment in order to help assess and ensure operational reliability. However, where operational or security considerations restrict the use of NC2 equipment for training or exercises, a capability shall be developed to simulate that equipment as realistically as possible. Training and exercises shall be conducted in a manner that poses no significant risk that these activities might be misinterpreted as evidence of hostile intent.

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E5. ENCLOSURE 5 (U)

ADDITIONAL POLICY REGARDING NCCS COMMUNICATIONS (U)

(b)(1)



~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E.5.3 (U) In compliance with DoD Directive 8100.1 (reference (z)), the GIG shall support all DoD missions with information technology for national security systems, joint operations, joint task force, and/or combined task force commands, that offers the most effective, efficient, assured information handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices.

E.5.4. (U) The Department of Defense shall, in compliance with reference (r), ensure that wireless devices, services, and technologies that are integrated or connected to DoD networks are considered part of those networks, and comply with Information Assurance guidance and accreditation rules contained in references (f), (q), and (s).

~~SECRET~~

~~SECRET~~

DoDD S-5210.81, August 8, 2005

E6. ENCLOSURE 6 (U)

ADDITIONAL POLICY REGARDING SAFETY, SECURITY, AND CONTROL
OF NUCLEAR WEAPONS (U)

(b)(1)



~~SECRET~~

(b)(1)