Department of Defense

# DIRECTIVE

**NUMBER** 5250.01
January 31, 2008

USD(I)

SUBJECT: Management of Signature Support Within the Department of Defense

References: (a) Title 10, United States Code
(b) "Transformation Planning Guidance," April 2003[1]
(c) "The National Security Strategy of the United States of America," March 2006[2]
(d) "The National Defense Strategy of the United States of America," March 2005[3]
(e) through (r), see Enclosure 1

## 1. PURPOSE

This Directive:

1.1. Establishes policy for the Signature Support Mission (SSM) within the Department of Defense pursuant to Reference (a).

1.2. Supports the Transformation of the Force in accordance with References (b) through (d); "The National Intelligence Strategy of the United States: Transformation through Integration and Innovation" (Reference (e); and the "Quadrennial Defense Review Report" (Reference (f)) by standardizing the signatures collection, processing, development, storage, maintenance, and dissemination processes to achieve the highest degree of efficiency and effectiveness in response to validated DoD requirements.

1.3. Assigns responsibilities for the oversight, management, and execution of the DoD SSM as defined within this Directive.

1.4. Establishes and promotes DoD SSM objectives:

[1] Available at http://www.oft.osd.mil/library/library_files/document_129_Transformation_Planning_Guidance_April_2003_1.pdf.
[2] Available at http://www.whitehouse.gov/nsc/nss/2006.
[3] Available at http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf

1.4.1. To provide precise, timely, high quality standardized signature data that allows applications to accurately identify equipment, activities, individuals, and events. Signature data must meet universal data tagging standards and use machine-understandable information templates to be effective in dynamic operational environments and facilitate sensor-to-shooter connections.

1.4.2. To maintain cognizance of advanced and emerging signature-related technologies for DoD system acquisitions and their associated signature content and fidelity, as well as to retain currency with state-of-the-art signature capabilities-based sensing.

1.5. Establishes a Senior Signature Management Forum (SSMF), comprised of general or flag officer (G/FO), Senior Executive Service (SES), or equivalent representatives, that provides policy, guidance, and priorities to the SSM.

## 2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of 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").

2.2. Applies to signatures of all equipment, activities, and events regardless of acquisition category to include, but not limited to, signatures utilized for intelligence, targeting, combat identification (CID), Blue Force tracking (BFT) and other tracks, smart munitions, training, weapons systems, and weapons system development. This Directive is not applicable to signatures as defined by the DoD Privacy Program per DoD Directive 5400.11 (Reference (g)).

## 3. DEFINITIONS

3. DEFINITIONS. Terms used in this Directive are defined in Enclosure 2.

## 4. POLICY

It is DoD policy that:

4.1. The Department shall have standardized signatures collection, processing, development, storage, maintenance, and dissemination processes to achieve the highest degree of efficiency and effectiveness within a net-centric enterprise information environment as defined in DoD Directive 8320.02 (Reference (h)) in response to validated DoD requirements.

4.2. Life-cycle signature support plans shall be established for validated and approved signature dependent programs and shall be developed during the concept refinement and technology development phases. They shall be fully defined prior to pre-Milestone B, as defined in DoD Directive 5000.1 (Reference (i)) and DoD Instruction 5000.2 (Reference (j)), and verified throughout the acquisition process.

4.3. All signature holders or developers shall maintain classification authority over their respective signature holdings. All signature holders or developers shall verify and document that all signatures and associated metadata submitted for inclusion in the DoD signatures pool have been reviewed for release to other countries in accordance with DoD Directive 5143.01 (Reference (k)) as applicable, Director Central Intelligence Directive 6/7 (Reference (l)), DoD 5200.1-R (Reference (m)), DoD Directive 5230.11 (Reference (n)), and "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (Reference (o)).

4.4. All signatures produced for the Department of Defense shall be made available through a distributed DoD signature pool and adhere to a set of SSMF-established signature standards.

## 5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)), in accordance with Reference (h), shall:

5.1.1. Serve as the DoD focal point for coordination and resolution of SSM issues involving non-DoD entities pursuant to Reference (k).

5.1.2. Develop policy and guidance and maintain intelligence management and security policy oversight regarding the SSM in accordance with Reference (k).

5.1.3. Oversee the SSM with respect to intelligence, surveillance, and reconnaissance (ISR) sites and platforms; measurement and signatures intelligence; and other areas as assigned in Reference (k).

5.1.4. Assign G/FO, SES, or equivalent representation to the SSMF established under this Directive.

5.1.5. In collaboration with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), establish intelligence program guidance priorities to address validated SSM requirements for current and future DoD ISR signature-dependent systems; issue implementing instructions and publish signature standards, as required.

5.2. The Director, Defense Intelligence Agency, under the authority, direction, and control of the USD(I), shall:

5.2.1. Establish a National Signatures Program (NSP) to manage and execute the SSM to accomplish the policy objectives of section 4 of this Directive.

5.2.2. Establish, maintain, and operate a single access point for the standardized distributed national signatures pool within each security domain, with multinational partners, other Federal agencies, and State and local governments, in accordance with law, policy, and security classification as defined in Reference (h).

5.2.3. Chair a dedicated SSMF.

5.3. The USD(AT&L) shall:

5.3.1. As the DoD Acquisition Executive pursuant to Reference (i), implement the policies outlined in section 4, as reflected in References (i) and (j) and addressed during systems acquisition processes, as appropriate.

5.3.2. Require that new acquisition programs identify, capture, and address the signatures essential to the development, testing, fielding, operation, and maintenance of required weapons, smart munitions, sensors, and systems capabilities at each program milestone and prior to proceeding to the Low-Rate Initial Production (LRIP), production and/or fielding decision.

5.3.3. Incorporate signature support requirements and funding into the Acquisition Strategy for both development and life-cycle support and provide to the SSMF.

5.3.4. Provide effective coordination between the NSP and the Defense Acquisition Community as deemed necessary for development of signatures.

5.3.5. Assign G/FO, SES, or equivalent representation to the SSMF.

5.3.6. In collaboration with USD(I) and the Chairman of the Joint Chiefs of Staff, establish priorities regarding the execution of the SSM to the Defense Acquisition Community to provide signature efficiency and effectiveness in response to validated DoD signature requirements.

5.3.7. Require that SSM requirements that include U.S., allied, or coalition signatures are adequately addressed in developmental testing programs and verified for compliance during operational test and evaluation.

5.4. The Under Secretary of Defense for Policy (USD(P)) shall develop and coordinate policy for identity management and disclosure of signature information pursuant to DoD Directive 5111.1 (Reference (p)).

5.5. The Director, Operational Test and Evaluation, shall consider the effects of the SSM during an acquisition systems' operational effectiveness and operational suitability evaluation.

5.6. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer shall:

5.6.1. Provide DoD acquisition programs with broad and consistent enterprise level implementation guidance so that systems developed by independent acquisition programs create a working net-centric enterprise information environment for dynamic signature operations.

5.6.2. Develop and coordinate policy of signatures utilized in Smart Card Technology per DoD Directive 8190.3 (Reference (q)).

5.7. The Chairman of the Joint Chiefs of Staff shall:

5.7.1. Incorporate signature requirements within the Joint Capabilities Integration Development System per Chairman of the Joint Chiefs of Staff Instruction 3170.01F (Reference (r)).

5.7.2. In coordination with the USD(AT&L), establish CID and BFT program guidance priorities to address validated SSM needs of current and future DoD CID/BFT signature-dependent systems.

5.7.3. Represent the interests and integrate the requirements of the Combatant Commanders.

5.7.4. Assign G/FO, SES, or equivalent representation to the SSMF.

5.8. The Heads of the DoD Components shall:

5.8.1. Participate in the development of the SSMF standards, implement the standards, and make available all signatures in the DoD signatures pool to authorized DoD and intelligence community users.

5.8.2. Execute and comply with SSM policy and guidance.

5.8.3. Require that Milestone Decision Authorities enforce compliance with SSM policy and guidance during the acquisition of signature-dependent programs and maintain classification authority over signature holdings obtained during acquisition.

5.8.4. Require that their organizations adhere to SSM requirements during the fielding of new systems, subsystems, and equipment and maintain classification authority over their respective signature holdings.

5.8.5. Identify at each program milestone, and prior to proceeding to the LRIP, production, and/or fielding decision, the signatures essential to the development, testing, fielding, operation, and maintenance of required weapons, smart munitions, and systems capabilities.

5.8.6. Identify, prioritize, and provide to the SSMF their organization's operational signature requirements for dynamic signature operations.

5.8.7. Identify and program, as part of the acquisition strategy, signature support requirements and funding for development and life-cycle support and provide to the SSMF.

5.8.8. Provide the SSMF notice of signature collections in order to maximize the sharing of collection opportunities among other DoD activities.

5.8.9. Assign G/FO, SES, or equivalent representation to the SSMF.

6. RELEASABILITY. UNLIMITED. This Directive is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This Directive is effective immediately.

Gordon England

Enclosures - 2
- E1. References, continued
- E2. Definitions

## E1. ENCLOSURE 1

## REFERENCES, continued

(e) "The National Intelligence Strategy of the United States: Transformation through Integration and Innovation," October 2005[4]
(f) "Quadrennial Defense Review Report," February 6, 2006[5]
(g) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007
(h) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004
(i) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003
(j) DoD Instruction 5000.2, "Operation of the Defense Acquisition System," May 12, 2003
(k) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(l) Director Central Intelligence Directive (DCID) 6/7, "Intelligence Disclosure Policy (U)," April 20, 2001[6]
(m) DoD 5200.1-R, "Information Security Program," January 14, 1997
(n) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(o) "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (NDP-1), October 2, 2000[7]
(p) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(q) DoD Directive 8190.3, "Smart Card Technology," August 31, 2002
(r) Chairman of the Joint Chiefs of Staff Instruction 3170.01F, "Joint Capabilities Integration and Development System," May 1, 2007

[4] Available from http://www.dni.gov/publications/NISOctober2005.pdf
[5] Available from http://www.defenselink.mil/pubs/pdfs/QDR20060203.pdf
[6] Available to authorized users of the SIPRNET from https://capco.dssc.sgov.gov/dcids_6.htm
[7] Provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense for Security Policy.

## E2. ENCLOSURE 2

## DEFINITIONS

For the purpose of this Directive, definitions are as follows:

E2.1. Blue Force Tracking. Employment of techniques to actively or passively identify and track U.S., allied, or coalition forces for the purpose of providing to the combatant commander enhanced battle space situational awareness and preventing fratricide to the maximum extent possible.

E2.2. Combat Identification. The process of attaining an accurate characterization of detected objects in the joint battle space to the extent that high confidence, timely application of tactical military options, and weapons resources can occur.

E2.3. DoD Signatures Pool. The virtual decentralized digital repository for DoD signatures for which the National Signatures Program provides authorized users a single point of entry and seamless online access for each security domain. The DoD signatures pool is a subset of the national signatures pool, which includes national, DoD, and Intelligence Community signatures.

E2.4. Dynamic Signature Operations. The provision of immediate, on-demand access to all sources of quality assured, standardized signatures and related data maintained within the Department of Defense.

E2.5. Life-Cycle Signature Support Plans. A management plan that is applied throughout the life of a signature-dependent acquisition that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of a signature-dependent acquisition.

E2.6. National Signatures Program (NSP). A joint multi-community federated program that provides users a horizontally integrated, seamless, online access to U.S. Government signature data. It leverages and links multiple signature data centers into a complementary distributed system through which signature users can readily locate and retrieve high-quality data. The Senior Signature Management Forum provides oversight, review, and guidance to the NSP.

E2.7. Senior Signature Management Forum (SSMF). A forum comprised of general or flag officer and Senior Executive Service or equivalent representatives from the Under Secretary of Defense for Intelligence; the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer; the Chairman of the Joint Chiefs of Staff; the Military Departments; and the Defense Intelligence Agency, the National Geospatial Agency, and the National Security Agency to oversee the execution of the Signature Support Mission. Provides overall policy, guidance, and priorities to the NSP.

E2.8. Signature. A distinctive basic characteristic or set of characteristics that consistently re-occurs and uniquely identifies a piece of equipment, activity, individual, or event.

E2.9. Signature-Dependent Defense Acquisition. A defense acquisition that utilizes or is comprised of a sensor, system, or process that relies on signatures or signature data to successfully perform a task or mission.

E2.10. Signature Provider or Developer. Any DoD organization that collects, processes, develops, and disseminates signatures for another organization within or outside the Department of Defense.

E2.11. Signature Support Mission. The life-cycle management of standardizing the signatures collection, processing, development, storage, maintenance, and dissemination processes to achieve the highest degree of efficiency and effectiveness in meeting DoD operational signature requirements. Includes the provision of a single access point for each security domain for all DoD signatures within the DoD signatures pool.