Department of Defense

INSTRUCTION

NUMBER 8410.03
August 29, 2012
Incorporating Change 1, July 19, 2017

DoD CIO

SUBJECT: Network Management (NM)

References: See Enclosure 1

1. PURPOSE. This Instruction, issued under the authorities of DoD Directive (DoDD) 5144.02 (Reference (a)) and DoDD 8000.01 (Reference (b)):

a. Establishes policy and assigns responsibility for planning, implementing, executing, and maintaining NM for the Global Information Grid (GIG) as an integral part of GIG Enterprise Management (GEM).

b. Supplements the overarching guidance for NetOps contained in DoD Instruction (DoDI) 8410.02 (Reference (c)) by directing that NM data be shared and that NM and spectrum management (SM) systems be integrated.

c. Supplements the guidance contained in DoDI 8500.01 (Reference (d)) by specifically requiring the adoption of mechanisms and processes for NM systems, (e.g., automated configuration management (CM) and policy based network management (PBNM) capabilities).

2. APPLICABILITY. This Instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

b. Applies to all DoD NM systems and associated technology, processes, personnel, and organizations that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, to include NM systems operated by a contractor or other entity on behalf of DoD and any NM system interfaces to DoD mission partners.

c. Shall not alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of sensitive compartmented information (SCI) and special access programs (SAP) for intelligence as directed by Executive Order 12333 (Reference (e)) and other laws and regulations. The application of the provisions and procedures of this Instruction to SCI or other SAP for intelligence information systems is encouraged where they may complement or discuss areas not otherwise specifically addressed.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. All NM systems shall be capable of distributed network control and facilitate net-centric sharing of network configuration, status, security, performance, utilization, and mission impact data with authorized users in accordance with (IAW) section 2 of Enclosure 3 of this Instruction.

b. Systems that use Simple Network Management Protocol (SNMP) shall use the latest version as the target protocol version IAW section 3 of Enclosure 3.

c. DoD Components operating NM systems shall develop service level agreements (SLAs) or similar agreements to ensure quality of service, interoperability, and availability of NM data exchanged between NM systems and with any authorized user IAW section 4 of Enclosure 3.

d. NM systems shall incorporate mechanisms or processes that ensure resiliency and continuity of operations in the event of a failure, loss, or disruption of NM capabilities due to a cyber attack or other manmade or natural occurrence.

e. NM systems shall have and use integrated automated CM and PBNM capabilities to improve DoD's ability to rapidly and consistently respond to cybersecurity events and maintain network availability and performance.

f. NM and SM systems shall be integrated, as appropriate, to create information technology (IT) resource management capabilities that provide the warfighter with enhanced situational awareness (SA) to support common understanding, planning, and monitoring; distributed network and spectrum control; and reduce life cycle costs.

g. NM interfaces to DoD mission partners (e.g., coalition and industrial suppliers) shall leverage and employ industry and commercial data standards, architectures, models, and exchange mechanisms to the maximum extent possible.

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 1. The changes to this issuance are administrative and update organizational titles and references for accuracy.

8. EFFECTIVE DATE. This Instruction is effective August 29, 2012.

Teresa M. Takai
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016
(c) DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008
(d) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(e) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(g) DoD Instruction 8320.02, "Sharing Data, Information, and Technology (IT) Services in the Department of Defense," August 5, 2013
(h) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015
(i) DoD Instruction 4650.01, "Policy and Procedures for Management and use of the Electromagnetic Spectrum," January 9, 2009
(j) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
(k) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, as amended
(l) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006
(m) Internet Engineering Task Force Request For Comment 2578, "Structure of Management Information Version 2 (SMIv2)," April 1999
(n) DoD Instruction 8320.05, "Electromagnetic Spectrum Data Sharing," August 18, 2011
(o) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended
(p) Memorandum of Agreement between the Assistant Secretary of Defense for Networks and Information Integration and the Intelligence Community (IC) Chief Information Officer for "Sharing Network Management and Computer Network Defense Information," June 24, 2005
(q) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
(r) Intelligence Community Directive 502, "Integrated Defense of the Intelligence Community Information Environment," March 11, 2011
(s) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and other Accountable Property," May 19, 2011
(t) DoDM 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012
(u) TeleManagement Forum, Information Framework (SID), GB922, Release 9.5
(v) Desktop Management Task Force, Common Information Model, version 2.31.1
(w) NIST Special Publication (SP) 800-126 rev2, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, Published: September 30, 2011
(x) DoD Discovery Metadata Specification, Version 4.0.1, November 11, 2011

(y) International Telegraph and Telephone Consultative Committee Recommendation X.731, "Information Technology – Open Systems Interconnection – Systems Management: State Management Function," January 1992
(z) International Telecommunication Union – Telecommunication Standardization Sector Recommendation M.3342, "Guidelines for the definition of SLA representation templates," July 2006
(aa) TM Forum GB917 Release 3.0, "SLA Management Handbook," January 2011
(ab) DISA Security Technical Implementation Guides, Network Infrastructure[1]
(ac) US Strategic Command Instruction 720-1, "Global Information Grid (GIG) NetOps Security Classification Guide (SCG)," July 15, 2009
(ad) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
(ae) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017
(af) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems & Networks," November 5, 2011, as amended
(ag) DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015
(ah) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition
(ai) Internet Engineering Task Force Request For Comment 2570, "Introduction to Version 3 of the Internet-standard Network Management Framework," April 1999

[1] http://iase.disa.mil/stigs/stig/index.html

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO, shall:

a. Provide strategy, policy, oversight, and guidance for NM capability, planning, definition, and implementation across the DoD Information Enterprise and GIG IAW Reference (b).

b. In coordination with Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and the Heads of the DoD Components, develop:

(1) End-to-end NM architectures and strategies that support efficient, effective, and secure NM operations in tactical and non-tactical networks and improve interoperability across NM systems.

(2) Mission-driven NM metrics for tactical and non-tactical networks and NM systems that enable consistent assessments of DoD network protection and performance.

(3) Strategies and architectures for IT resource management capabilities that efficiently and effectively integrate NM and SM systems across doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF).

c. Ensure that the Defense Information Systems Agency (DISA), in coordination with the other DoD Components, develops, coordinates, and establishes NM data schemas that facilitate the sharing of tactical edge NM information within tactical edge networks and with NM systems that manage non-tactical edge networks IAW DoDI 8320.02 (Reference (g)).

d. Ensure that NM data schemas, technical standards and specifications, interface definitions, and other related information are available to all authorized users from the DoD Metadata Registry (MDR), Defense Technical Information Center, or other appropriate websites and repositories.

e. Develop, in coordination with the Heads of the DoD Components, guidelines for network SLAs, a DoD service level management governance framework, and a process for reviewing and coordinating SLAs.

f. Develop, in coordination with the Heads of the DoD Components, NM records and information management and retention guidelines IAW DoDI 5015.02 (Reference (h)).

g. Ensure that NM and SM capabilities are acquired in coordination with USD(AT&L) and are managed, integrated, and synchronized consistent with Reference (b), and DoDIs 4650.01, 4630.08, and 5000.02 (References (i), (j), and (k)).

h. Develop, in coordination with the Heads of the DoD Components, architectures and standards for automated CM and PBNM capabilities based on the results of the USD(AT&L) assigned responsibilities contained in this Instruction.

2. DIRECTOR, DISA. The Director, DISA, under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in sections 8 and 9 of this enclosure and IAW DoDD 5105.19 (Reference (l)), and in coordination with the Heads of DoD Components, shall:

a. Establish and maintain repositories of NM data schemas, technical standards and specifications, interface definitions, and SNMP management information bases (MIBs) based upon security classifications, to include proprietary SNMP MIBs IAW the Internet Engineering Task Force Request For Comment 2578, "Structure of Management Information Version 2 (SMIv2)" (Reference (m)).

b. Develop and maintain, with support from the DoD Components, the definition of NM data exchanges, translations, and associated data schemas among all NM systems, to include tactical edge NM systems. This effort shall leverage and employ industry and commercial data standards, architectures, models, and exchange mechanisms to the maximum extent possible.

c. Define common data standards for sharing information and data between NM and SM systems IAW DoDI 8320.05 (Reference (n)).

d. Establish and maintain a standard dictionary for use in constructing standard NM data schemas for exchanging NM information between NM systems and for exposing NM data to non-NM systems.

e. Establish naming conventions and standards that facilitate the sharing of NM information and control capabilities among NM systems across established NetOps operational hierarchies and NM domains.

f. Establish and maintain definitions and interface control documents for standard mechanisms for exchanging NM information between NM systems and for exposing data to non-NM systems.

g. Create, manage, and maintain a common repository based upon security classifications within the MDR for all data-exchange schemas and SNMP MIBs used by NM systems, including supporting documentation and interface characteristics and specifications.

h. Participate in applicable standards bodies and organizations to advocate for and aid in developing standards, protocols, and mechanisms for translating NM information from current formats (e.g., SNMP) to ones that facilitate net-centric information sharing (e.g., extensible markup language).

i. Develop, in coordination with the DoD Components, a GIG technical profile (GTP) to define the interface specifications for exchanging data between NM systems.

j. Develop and promulgate DoD-wide standards and guidelines for use of NM protocols (such as SNMP or network configuration protocol) for communication of NM information between NM systems and their managed network elements (NEs).

k. Develop, in coordination with the Commander, U.S. Strategic Command (USSTRATCOM), technical guidance for integrating and correlating NM and SM capabilities to enable near real-time end-to-end network SA throughout the GIG.

l. Support the USD(AT&L) in reviewing and studying automated CM and PBNM capabilities and standards.

m. Develop and promulgate technical guidance and architectures for developing and implementing automated CM and PBNM systems.

n. Establish and maintain a central repository of SLAs.

3. USD(AT&L). The USD(AT&L) shall:

a. Provide coordination and support to ensure that any policies, guidance, or requirements proposed by the DoD CIO regarding SM and NM requirements impacting access to defense networks and vendor facing applications by members of the Defense Industrial Base (DIB) will not place any undue burdens on industry.

b. Prepare and coordinate acquisition and contracting policy, procedures, and regulation among DIB members and Federal partners necessary to implement this Instruction.

c. Coordinate with DIB members supplying materiel and services, to ensure an executable and affordable migration strategy to meet SM and NM requirements resulting from the implementation of this Instruction.

d. Implement automated CM and PBNM capabilities and standards in new or modified NM systems, including but not specifically limited to determining architectures and technical approaches for:

(1) Network traffic bandwidth prioritization.

(2) Contingency-based configuration changes that will satisfy a typical joint operation, including potential coalition partners or similar.

(3) Implementing automated configuration change technologies.

(4) Determining standard methods for human override of automated configuration changes.

4. DIRECTOR, OPERATIONAL TEST AND EVALUATION (DOT&E). The DOT&E shall:

a. Ensure processes, procedures, and infrastructure are available to operationally test and evaluate NM capabilities that are developed and acquired.

b. Conduct periodic assessments of NM processes, procedures, and capabilities as requested by the DoD CIO.

5. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I) shall serve as the DoD focal point to the Intelligence Community (IC) for NM policy and oversight matters relating to intelligence information sharing and interoperability of Defense intelligence systems and processes IAW DoDD 5143.01 (Reference (o)).

6. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I) and as the Manager of the SCI component of the GIG shall, in addition to the responsibilities in sections 8 and 9 of this enclosure, interact with the Director of National Intelligence to facilitate coordination and sharing of DoD SCI network status and SA information IAW the memorandum of agreement between the DoD CIO and the IC CIO (Reference (p)).

7. DIRECTOR, NATIONAL SECURITY AGENCY (DIRNSA)/CHIEF, CENTRAL SECURITY SERVICE (CHCSS). The DIRNSA/CHCSS, under the authority, direction, and control of the USD(I), in addition to the responsibilities in sections 8 and 9 of this enclosure, and, consistent with the National Manager responsibilities assigned to DIRNSA by National Security Directive 42 (Reference (q)), shall lead, with the support of the other DoD Components, the development of suitable technical standards; administrative guidance; key-management protocols, devices, and systems; encryption methods; and other items as required to enable NM systems and the NE they manage to comply with applicable security controls.

8. HEADS OF THE DEFENSE INTELLIGENCE COMPONENTS. The Heads of the Defense Intelligence Components shall execute their NM responsibilities consistent with Intelligence Community Directive 502 (Reference (r)).

9. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Execute NM within the portions of the Defense Information Enterprise within their assigned area of responsibility (AOR) IAW Reference (b) and in support of Combatant Commanders' responsibilities.

b. Support DoD CIO, USD(AT&L), Director, DISA, and Commander, USSTRATCOM (CDRUSSTRATCOM) in developing mission-driven metrics and end-to-end NM architectures

and strategies that support efficient NM operations in tactical and non-tactical networks to improve interoperability and integration across NM systems.

c. Develop strategies and architectures for IT resource management capabilities that efficiently, effectively, and securely integrate NM and SM systems across DOTMLPF.

d. Support DISA in developing and maintaining NM standards, specifications, and interfaces to include defining extensions to baseline NM data-exchange schemas necessary to enable and facilitate the exchange and sharing of NM information and data with tactical edge NM systems.

e. Implement common data-exchange schemas to ensure interoperability of NM systems sufficient to execute the SLAs or similar agreements IAW section 3 of Enclosure 3 of this Instruction. Individual NM systems may either directly implement the schemas or may provide translation to and from these schemas.

f. Plan, organize, procure, develop, test, implement, and operate NM capabilities within established NetOps operational hierarchies and NM domain structures.

(1) Support CDRUSSTRATCOM in the development and vetting of NM data standards and sharing mechanisms.

(2) Ensure Component NM systems comply with USSTRATCOM-approved NM data-exchange schemas and standards-based data sharing mechanisms.

(3) Ensure that new or modified NEs are discoverable, manageable, and comply with applicable security controls in accordance with Reference (d).

g. Support CDRUSSTRATCOM in establishing NetOps hierarchies that fully consider NM along with network defense and content management.

h. Support CDRUSSTRATCOM in developing operational requirements for automated CM and PBNM.

i. Ensure that NM systems are resilient to manmade or natural events that may cause failure, loss or disruption of NM capabilities.

j. As needed and with DISA support, develop standard NM information and data models to include NM MIB standards for tactical edge NEs.

(1) Standards shall consider the unique properties of tactical networking, including but not limited to the ad-hoc nature of such networks, the requirement for NEs to connect and disconnect at random due to mobility-related constraints, the often limited bandwidth available, and operational requirements to remain in a non-transmitting state for extended periods of time.

(2) Where appropriate, these standards shall be established jointly, maintained by DISA, and incorporated into the baseline schemas for NM.

k. Provide the NM and SM data necessary to fulfill the commander's critical information requirements in support of established DoD cyberspace operational hierarchies.

l. Ensure, in coordination with DISA, all DoD equipment containing or potentially containing personally identifiable information and other data of a sensitive nature is managed in accordance with DoDI 5000.64 (Reference (s)).

10. CJCS. The CJCS, in addition to the responsibilities in section 8 of this enclosure and in coordination with the other Heads of the DoD Components, shall:

a. Establish and issue priorities for the collection and sharing of NM data.

b. Develop and promulgate joint NM tactics, techniques, and procedures.

c. In coordination with the Combatant Commanders, establish requirements for sharing NM information and data with coalition partner networks.

11. COMMANDERS OF THE COMBATANT COMMANDS. The Commanders of the Combatant Commands, in addition to the responsibilities in section 8 of this enclosure, shall support the Joint Staff in establishing requirements for sharing NM information and data with coalition partner networks.

12. CDRUSSTRATCOM. The CDRUSSTRATCOM, in addition to the responsibilities in sections 8 and 10 of this enclosure, shall:

a. Develop and issue guidance for ensuring uninterrupted, end-to-end monitoring and control of all operational DoD networks.

b. Develop, publish, and enforce standard processes for the sharing of NM data about readiness and operating status of all DoD networks.

c. Establish clear lines of authority and responsibility for NM across all DoD network domains and with DoD mission partners.

d. Develop, in coordination with the Director, DISA, operational guidance for integrating and correlating NM capabilities to enable near real-time end-to-end network SA.

e. Develop, in coordination with the other Heads of the DoD Components, and issue security classification guidelines for NM and SM information IAW DoDM 5200.01, Volume 1 (Reference (t)).

f. Approve NM data schemas and sharing mechanisms.

g. Develop, in coordination with the other Heads of the DoD Components, automated CM and PBNM operational requirements.

ENCLOSURE 3

PROCEDURES

1. GENERAL. The procedures in this enclosure are applicable to all NM systems, including those intended for the tactical environment, except as specifically noted in each section.

2. NM DATA EXCHANGE GUIDELINES

a. The DoD shall adopt and implement the TeleManagement (TM) Forum Information Framework (formerly known as the Shared Information and Data Model) and the Desktop Management Task Force (DMTF), Common Information Model (CIM) as the foundation NM information and data models and the National Institute of Standards and Technology (NIST) Security Content Automation Protocol as the baseline protocol and standards for sharing security management information sharing (References (u), (v), and (w)). Drawing on the DISR, other industry-standard information and data models (e.g., Internet Engineering Task Force (IETF), DMTF CIM, IETF SMIv2) and protocols (e.g., International Telecommunications Union-Telecommunication Cybersecurity Information Exchange (ITU-T CYBEX)) may be used to tailor those baselines where application requirements and other circumstances so warrant. Only if existing standards cannot be extended shall DoD Components adopt and implement non-standards based data schemas and exchange mechanisms.

b. The CDRUSSTRATCOM, IAW Reference (c) and functioning IAW Reference (g), shall vet and approve NM data schemas and sharing mechanisms.

c. DoD programs of record (POR) shall adopt and implement NM data schemas and net-centric sharing mechanisms that have been approved by CDRUSSTRATCOM. In situations where it is determined that adopting approved NM data schemas and net-centric sharing mechanisms would result in unacceptable delay or increased costs to a POR, a request for waiver will be submitted via the applicable acquisition oversight process.

(1) Where standards or data schemas are not available or have not been approved, program offices shall work with DISA to identify and vet program specific data standards, schemas, and exchange mechanisms prior to them being submitted to CDRUSSTRATCOM for approval.

(2) Requests for approval of data schema or sharing mechanism submitted to USSTRATCOM must be reviewed and adjudicated within 90 days of their submittal to ensure that program development timelines should not be adversely impacted.

d. NM systems shall use Enterprise Services (ES) that have been approved by the DoD CIO to enable and facilitate the discovery, sharing, and collaborative use of NM data among all authorized users.

e. All approved NM data-exchange schemas shall be registered in the DoD MDR to include associated metadata schemas and discovery metadata and shall be made available to all DoD Components and authorized mission partners.

(1) NM data elements shall be made visible by creating and associating metadata (referred to as "data tagging"), including discovery metadata.

(2) Discovery metadata shall conform to the DoD Discovery Metadata Specification (Reference (x)).

(3) DoD metadata standards shall comply with applicable national and international consensus standards for metadata exchange whenever possible IAW Reference (g).

(4) All metadata shall be discoverable, searchable, and retrievable using DoD-wide capabilities.

(5) Metadata shall include the classification level of each NM data element.

(6) Metadata shall be classified when any single item of metadata or a compilation of metadata meets the requirements for classification, IAW Reference (t).

f. NM data-exchange schemas shall identify and define similar or identical parameters in the same way. Resolution of parameter naming and definition shall be the responsibility of CDRUSSTRATCOM working in coordination with other affected community of interests.

g. The specific data and information available from an NM system varies based on system capabilities and implementation but at a minimum NM systems should be capable of collecting and reporting the following information about the NEs they manage:

(1) Operational configuration.

(2) Current operational state.

(3) Current usage state.

(4) Available NE capacity and percent of capacity currently committed.

h. NE data will normally be collected through the device's MIB values for SNMP managed devices or by other means for non-SNMP managed devices and the resulting information shall be shared with authorized users via an ES or other net-centric data sharing mechanism.

i. The CDRUSSTRATCOM, in coordination with DISA and the DoD Components, shall define a minimum set of standards and values for reporting information based on International Telegraph and Telephone Consultative Committee (CCITT) Recommendation X.731 (Reference (y)) and other applicable IETF, Distributed Management Task Force, and TM Forum standards.

3. NM USE OF SNMP

a. All SNMP MIBs used in the DoD shall comply with technical standards in the DISR and DISA Security Technical Implementation Guides (STIGs).

b. All MIBs along with full descriptions of their use and format shall be stored in an MIB registry managed and published by DISA.

c. Where possible, elements in multiple MIBs that refer to the same parameter shall be formatted and identified the same way. Standard formats and identifications shall be maintained in a DoD-published MIB data format and dictionary established and maintained by DISA.

d. New SNMP managed resources and management applications shall use the latest approved version of SNMP, to take advantage of the additional security features provided with this version of the protocol. Existing systems that use SNMP shall transition to the latest approved SNMP version when feasible.

e. The latest version of SNMP shall be implemented with a security model appropriate to the security of the network rather than the default model.

f. Existing systems that use SNMP v1 or v2c shall implement the following security precautions in the period prior to transition to the latest approved version of SNMP:

(1) NEs requiring SNMP management shall be properly configured with appropriate read-only and read-write community names (commonly referred to as "community strings").

(2) Read-only and read-write SNMP community strings for a managed device shall be different.

(3) Where possible, a different string (or strings) shall be utilized for each NE, or at minimum for each area of the network being managed. For instance, if an authorized user requests access to information about DISN, they could be given a read-only community string and a list of devices that it can be used to access. In addition to enabling access, this approach allows network managers to quickly and easily isolate portions of the network and serves to keep the number of required community strings to a manageable level.

(4) SNMP community strings shall be safeguarded and protected against compromise at the level of the operational network.

(5) SNMP community strings shall meet the minimum password length and composition requirements required by applicable security controls.

(6) The community strings and management passwords shall be changed at least annually and when there is a possibility that one has been compromised.

(7) The community strings shall be modified from default settings – default "public" and "private" strings shall not be utilized.

(8) Periodic SNMP polling should be done with a read-only community string, and read-write strings should be used only for write operations, based on the capabilities of the NM system.

(9) Unauthorized attempts to access SNMP managed NE shall be aggressively monitored and reported.

(10) Device, account, and application passwords will not be passed over SNMP until the transition to the latest version is accomplished.

g. Access control lists shall be implemented on SNMP managed NEs, where possible, to restrict access to only authorized NM operators and NM systems.

4. SLAs

a. NM systems shall be located within the network topology in a manner that ensures they can monitor and report on SLA compliance.

b. NM SLAs shall at a minimum address the following areas identified in International Telecommunications Union – Telecommunications Recommendation M.3342 (Reference (z)) and TM Forum GB917 Release 3.0 (Reference (aa)):

(1) Identification of the organizations between which the agreement is established, to include technical and organizational points of contact.

(2) A description of the NM services that will be provided along with scope, limitations, and other terms of reference that might be needed.

(3) A basic description of the NM system and supporting equipment information and who is responsible for providing, maintaining, and operating it.

(4) Detailed explanations of the expected levels and quality of NM services that will be provided.

(5) How NM service levels will be monitored and reported. This section must include: where, how, and in what format NM information and data will be collected; how often it will be collected; how it will be shared with the customer; how often it will be shared with the customer; how NM information and data will be archived; and duration archived information will be retained IAW Reference (h). This section will define for all parties:

(a) The characteristics of the NM information to be exchanged (e.g., data schema(s) used, specialized data formatting (if any), and any non-standard characteristics).

(b) Required NM data update rates.

(c) Maximum allowable time from when an event takes place to when it is reported by the NM system, as well as the location of event.

(d) Location of the NM event.

(e) Allowable NM system initialization time and data sync (or data re-sync due to NM and radio reconnection).

(f) Required local event storage requirements (if any).

(g) Reporting formats, destinations, and update rates (if finished reports are to be provided.

(h) Mechanisms for enforcement, auditing, and assurance.

(6) A description of NM system backup, recovery and continuity of operations requirement.

(7) Procedures for changing and terminating the SLA.

(8) A description of the remedies available to the customer in the event the NM system does not perform as agreed.

c. SLAs and other agreements that include tactical edge and non-tactical edge networks shall take into consideration the unique characteristics of tactical edge networks (e.g., dynamic, ad-hoc, bandwidth constrained, and intermittent connections); however these characteristics shall not be used to exempt tactical edge and non-tactical edge networks from the requirement to have SLAs. Implementation of SLAs for tactical edge and non-tactical edge networks shall not impact network or mission effectiveness.

d. NM SLAs and other agreements shall be structured to complement or extend other SLAs entered into by DoD Components. If desired, an NM SLA or equivalent could be made part of the overall SLA, or similar agreement addressing the networks being managed.

e. NM SLAs and other agreements shall establish baseline and minimum service levels and address provisioning and measurement of the following network performance parameters:

(1) Network latency and packet loss on per-hop and end-to-end basis by traffic type.

(2) Minimum and maximum bandwidth provided.

(3) Mean time between failures of network equipment or connectivity.

(4) Mean time to repair failures in network equipment or connectivity.

(5) Throughput of a given network node, by traffic type.

(6) Percentage of available bandwidth consumed on a given link, by traffic type.

(7) Fault status, by node priority.

(8) Packet error rate and bit error rate (average and standard deviation) through a given network node.

(9) Quality of service requirements for NM and control plane traffic.

5. NM SECURITY

a. Data exchanges between NM systems shall be encrypted per DISA Security Technical Implementation Guides Network Infrastructure (Reference (ab)) and shall be processed and protected at the appropriate classification level.

b. Management information obtained from NEs shall be classified, stored, processed, and shared IAW the USSTRATCOM GIG NetOps Security Classification Guide (Reference (ac)) and other applicable classification guides. NM data that provides sensitive operational status of the network or the status of the network's ability to support real-world operations shall be protected as sensitive information (minimum) or at an appropriate higher classification level based on the classification of the network it is derived from.

c. NM system operator and supervisory positions (e.g., system administrators, network managers and controllers, router and switch administrators, managers and controllers) performing NM IA functions as defined in DoD 8570.01-M (Reference (ad)) shall be designated IA Technical Category Level 2 and IA Management Category Level 2 positions and as critical sensitive positions as defined by DoD 5200.2-R (Reference (ae)), and military, government civilian, and contractor personnel filling them shall meet all required background checks, training, and certification requirements prior to assuming their duties.

d. Access to NM systems shall be authorized by the appropriate unit level commander responsible for the NM system. Only those users with proper credentials and access authorizations will be granted access to NM systems. NM system users shall comply with the applicable cybersecurity training and certification requirements IAW Reference (ad).

e. NM functions are critical within the network infrastructure. Accordingly, supply chain risk management shall be applied to the acquisition of NM functionality IAW DoDI 5200.44 (Reference (af)) and DoDI 5200.39 (Reference (ag)).

6. NM STANDARDS AND SCHEMAS FOR TACTICAL EDGE NE. To support end-to-end SA and NM system reporting criteria, common NM standards are required to support spectrum-dependent systems and tactical edge NEs.

a. In consideration of tactical edge NM requirements, the DoD Components with DISA support shall jointly establish NM standards for tactical edge NEs. The standards shall be maintained by DISA and incorporated into the baseline schemas for NM. These standards shall consider the unique properties of tactical networking, including but not limited to:

(1) The ad-hoc nature of such networks.

(2) The requirement for NEs to connect and disconnect at random due to mobility-related constraints.

(3) The often limited bandwidth available.

(4) Operational requirements to remain in a non-transmitting state for extended periods of time.

b. As requested, DISA shall support program managers, in the incorporation of these standards into new or existing programs of record.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AOR	area of responsibility
CCITT	International Telegraph and Telephone Consultative Committee
CDRUSSTRATCOM	Commander, U.S. Strategic Command
CHCSS	Chief, Central Security Service
CIM	Common Information Model
CJCS	Chairman of the Joint Chiefs of Staff
CM	configuration management
CYBEX	Cybersecurity Information Exchange
DIA	Defense Intelligence Agency
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DMTF	Desktop Management Task Force
DoDD	DoD Directive
DoDI	DoD Instruction
DOT&E	Director, Operational Test and Evaluation
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel and facilities
DoD CIO	DoD Chief Information Officer
ES	Enterprise Services
GEM	GIG Enterprise Management
GIG	Global Information Grid
GTP	GIG technical profile
IAW	in accordance with
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	information technology
ITU-T	International Telecommunications Union-Telecommunication
JCIDS	Joint Capabilities Integration and Development System
MDR	Metadata Registry
MIB	management information base
NE	network elements
NETCONF	Network Configuration Protocol
NIST	National Institute of Standards and Technology
NM	network management
NSA	National Security Agency
PBNM	policy based network management
POR	programs of record
RFC	Request For Comment
SA	situational awareness
SAP	special access programs
SCI	sensitive compartmented information
SLA	service level agreement
SM	spectrum management
SMIv2	Structure of Management Information Version 2
SNMP	Simple Network Management Protocol
STIG	Security Technical Implementation Guide
TM Forum	TeleManagement Forum
USD(I)	Under Secretary of Defense for Intelligence
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USSTRATCOM	U.S. Strategic Command

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for purposes of this Instruction.

Defense Intelligence Components. Defined in Reference (o).

distributed network control. Describes network and other types of monitoring, management, and control systems where the monitoring, management, or control elements are not centrally located but rather distributed throughout the system or systems being managed thereby providing the capability for each managed NE to be controlled by more than one NM system. The exact policies and procedures for determining which NM systems is in control of a particular managed NE at any given time will be as directed by applicable policies and guidelines.

DoD Information Enterprise. Defined in Reference (b).

end-to-end SA. Comprehensive visibility and awareness across all links or elements in a network connectivity chain.

ES. Any capability provided for broad use across the DoD that enables awareness of, access to or delivers information across the GIG.

GIG. Defined in Reference (b).

GIG SA. Defined in Reference (c).

GEM. Defined in Reference (c).

GTP. A description of required operational functionality and technical specifications for using and interfacing GIG ES. A GTP has: (a) an interoperability reference architecture and service description section that has an interoperability reference architecture and graphic and a service description; (b) an interoperability requirements and secured availability section; (c) a technical implementation profile for critical GIG technical standards and interfaces that are part of the GTP; (d) a maturing guidance section; a compliance testing section; (e) a key programs implementing the GTP section; (f) a data section; and (g) a references section.

Integrated IT Resource Management System. The single set of integrated technical capabilities and processes that enable the deployed warfighter to efficiently and effectively plan, deploy, monitor, control and recover communications, EW, radar, networking, spectrum, navigation, satellite systems and assets across all tactical edge networks and operating environments.

MIB. Defined in Reference (m).

mission partners. Defined in Reference (c).

NE. A piece of telecommunications equipment that provides support or services to the user. This includes the components or devices that make up a network and communicate via wired or wireless mediums with NM systems.

NetOps. Defined in Reference (c).

network. A set of routing, switching, load balancing, security, and transmission subsystem communications components. Networks can be Internet Protocol (IP) based, non-IP based, or a combination. Networks can be wired, wireless, terrestrial, airborne, seaborne, satellite, or based on a combination of transport mechanisms and protocols. A network includes all hardware, firmware, and software components residing in routing, switching, load balancing, security and transmission subsystem communications components themselves, as well as any communications-related hardware, firmware, and software components that reside in supporting hosts (e.g., communications protocols).

network provider. The organization that maintains and operates the network components required for intelligent network functionality.

NM. The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating and monitoring the resources of a telecommunications network, including performing functions such as initial network planning frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, CM, fault management, security management, performance management, and accounting management. NM does not include user terminal equipment.

NM data. Includes raw data that is collected from managed NEs and used by a NM system to determine and report their status, configuration, etc. and processed NM information that is based on or derived from the raw data and that is intended for sharing beyond the element management level.

An example of raw data would be information collected from a router or host using SNMP.

An example of processed information would be a trouble ticket that is used to share outage information with another NM system.

NM domain. A group of networks and their component NEs and management systems that operate under common rules and procedures, typically under the control of a single organization.

NM system. The integrated collection of NM hardware, software, and processes that facilitate the collection and exchange of network information through monitoring, controlling, configuring, and allocating resources through common or translated protocols and MIB mapping.

PBNM. Using set of rules (also referred to as policies) to manage the state of the network by directing managed elements (e.g., routers) to perform certain actions on network devices to tune their performance, configuration, and/or behavior.

situational or situation awareness (also called GIG SA). Defined in Reference (c).

SM. (Also known as electromagnetic SM). Defined in the DoD Dictionary of Military and Associated Terms (Reference (ah)).

SNMP. Defined in IETF Request for Comment 2570 "Introduction to Version 3 of the Internet-standard Network Management Framework" (Reference (ai)).

tactical edge NM systems. Those NM systems that operate within the approximate first tactical mile for joint forces connected to the GIG, which includes a variety of wired and wireless networks.

telecommunications management network. An architecture for management, including planning, provisioning, installation, maintenance, operation and administration of telecommunications equipment, networks, and services.

vendor-facing applications. A software program within an automated information business system performing DoD acquisition missions that provides for controlled access for solicitation information, contract award information, and payment and contract administration purposes to the vendors specifically listed in the Central Contractor Registration (CCR) who have been awarded contracts by the Federal Government.