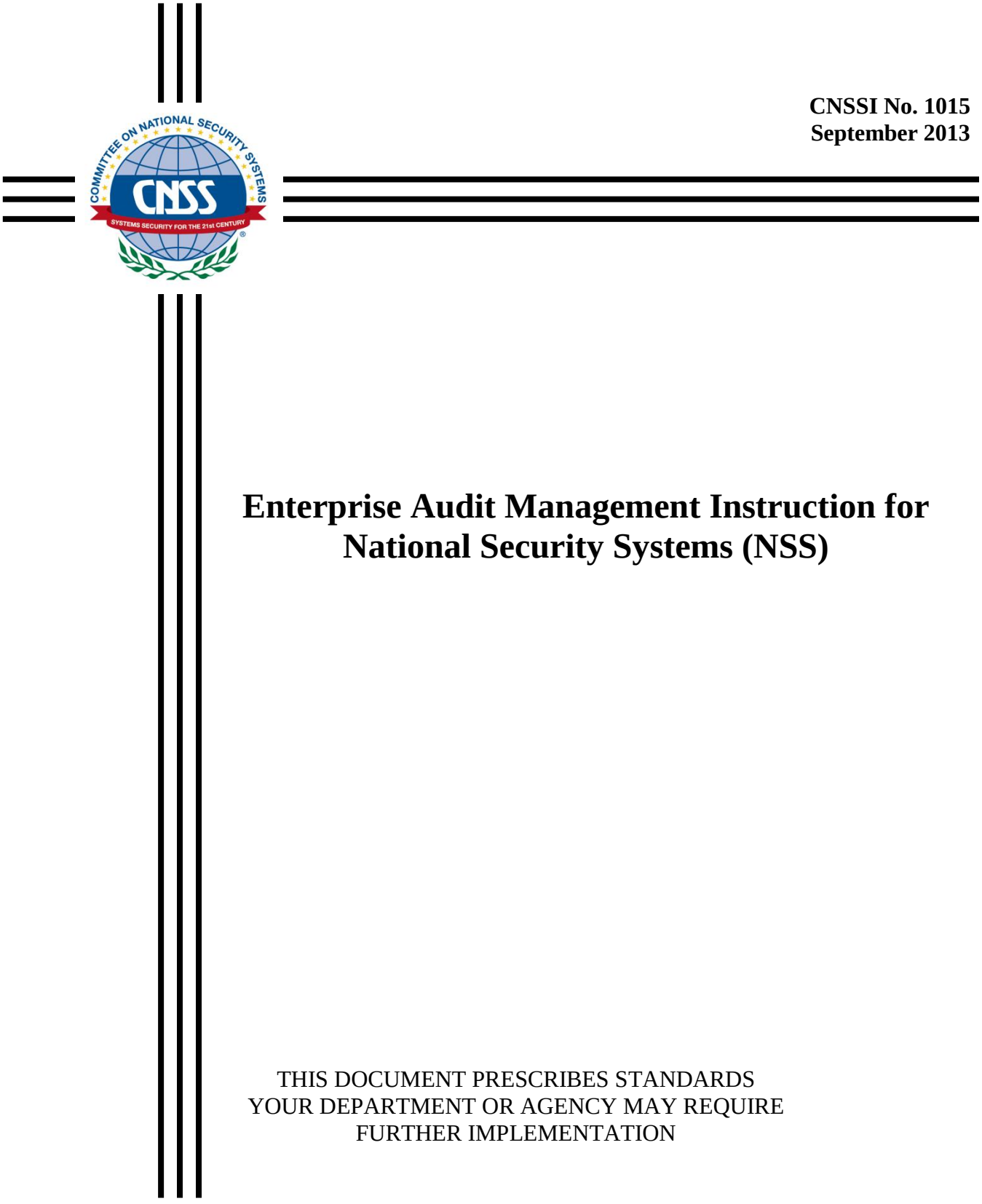

CNSSI No. 1015
September 2013

Enterprise Audit Management Instruction for National Security Systems (NSS)

THIS DOCUMENT PRESCRIBES STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE
FURTHER IMPLEMENTATION

NATIONAL MANAGER

FOREWORD

1. The Committee on National Security Systems Instruction (CNSSI) No. 1015, *Enterprise Audit Management (EAM) Instruction for National Security Systems (NSS)* provides operational guidance and assigns responsibilities for deploying EAM for National Security Systems. It establishes the minimum national requirements for an Enterprise Audit Management program within the national security community and provides a framework for decision makers to continuously monitor asset integrity, manage risk in order to maintain system security, and develop meaningful enterprise situational awareness (SA). EAM applies the general concepts, processes, and activities of audit management with a focus on outcomes that affect the security posture of the information system via automation.

2. This Instruction presents a phased approach to automation that aids in the implementation of the security controls required by CNSSI No. 1253, *Security Categorization and Control Selection for National Security Systems* (Reference a), and assists in resource prioritization. Annex B of this Instruction contains the Capability Maturity Compliance Model (CMCM) and automated EAM requirements. Automated EAM maturity level compliance is achieved by implementing the EAM security controls via automated means (e.g., automated tools, processes, and process support).

3. Compliance with this Instruction must be achieved through the application of the Risk Management Framework found in CNSSP No. 22, *Policy for Information Assurance Risk Management for National Security Systems.*

4. NSS owners are responsible for implementing this Instruction in a manner that supports organizational continuous monitoring efforts and the risk management framework as defined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* (Reference c).

5. It is anticipated that the NIST SP 800-53 security controls and CNSSI No. 1253 baselines will evolve as technology evolves and automation becomes more pervasive. As such, this Instruction will periodically be reviewed and revised accordingly.

6. Additional copies of this Instruction are available at the address listed below.

FOR THE NATIONAL MANAGER

/s/

DEBORA A. PLUNKETT

TABLE OF CONTENTS

SECTION **PAGE**

SECTION I – PURPOSE 1
SECTION II – AUTHORITY 1
SECTION III – SCOPE 1
SECTION IV – POLICY 1
SECTION V – RESPONSIBILITIES 2
SECTION VI – DEFINITIONS 3
SECTION VII – REFERENCES 3
ANNEX A – CAPABILITY MATURITY COMPLIANCE MODEL (CMCM) A-1
ANNEX B – SET OF AUDITABLE EVENTS B-1
ANNEX C – DEFINITIONS C-1

ENTERPRISE AUDIT MANAGEMENT
FOR
NATIONAL SECURITY SYSTEMS

CNSSI 1015

SECTION I – PURPOSE

1. Committee on National Security Systems Instruction (CNSSI) No. 1015 details the minimum national requirements and assigns responsibilities for deploying Enterprise Audit Management (EAM) capabilities for National Security System (NSS) as defined in Annex A. This Instruction is a derivative issuance of Committee on National Security Systems Directive (CNSSD) No. 502, *National Directive on National Security Systems* (Reference d).

SECTION II – AUTHORITY

2. The authority to issue this Instruction derives from National Security Directive No. 42, *National Policy for the Security of National Security Systems* (Reference e), that outlines the roles and responsibilities for securing National Security Systems, consistent with applicable law, Executive Order (E.O) . 12333, *United States Intelligence Activities* (Reference f), as amended, and other Presidential directives.

3. Nothing in this Instruction alters or supersedes the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This Instruction establishes the minimum automated EAM standards required for Department and Agencies (D/As) with NSS. It complements other CNSSIs that, when integrated across all NSS, will help protect, detect, defend, and manage NSS, as well as enhance situational awareness.

5. Upon final signature of this instruction, the controls invoked within the body of this document will be published in the CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*, Low-Low-Low baselines within 90 days as an administrative update.

SECTION IV – POLICY

6. EAM is important not only in securing assets, but also in provisioning for computer network defense and ultimately providing overall situational awareness of both the activities occurring on NSS assets and the security posture of the enterprise. Adherence to this Instruction

and the audit management techniques promulgated by the National Manager are mandatory for all users of NSS.

7. Whenever conflicting CNSS EAM implementing directives are encountered, this Instruction will take precedence.

8. A mature EAM program must provide a comprehensive, automated capability optimized to protect NSS. An EAM program must provide owners and operators with awareness of, and the ability to respond to, the insider threat, the threat from remote adversaries, and the threat from non-malicious activities that can impede the mission. Security audit trails must provide the means to accomplish a number of broad security and mission objectives:

a. Unique identification and accountability of individuals using IT resources (insider)
b. Identification of unauthorized activity from any source (intrusion)
c. Recorded evidence of system activity (forensics)

9. D/A must share, where lawful and appropriate, audit data identified in Annex B – Set of Auditable Events to support Information Assurance, business analytics, personnel security, and other community audit needs related to NSS information resources.

SECTION V – RESPONSIBILITIES

10. D/As must plan, implement, and manage automated EAM activities for their NSS in accordance with the guidance provided in this Instruction and in consultation with their respective legal counsel and civil liberties and privacy officials. D/As may implement more stringent audit management requirements than those included in this Instruction as necessary to support their respective missions.

11. D/As must configure and implement audit management capabilities to effectively protect and defend NSS; therefore, heads of D/As must implement, at a minimum, automated management and technical security capabilities for EAM, as outlined in Annex A - Capability Maturity Compliance Model (CMCM).

12. D/As must conduct self assessments to demonstrate compliance with CMCM guidance.

13. The authorizing official (AO) is responsible for making risk decisions in support of the automated EAM, using the Risk Management Framework found in CNSSP No. 22, and the selection of applicable security controls in accordance with CNSSI No. 1253.

14. D/As must integrate automated EAM with the organizational continuous monitoring efforts.

SECTION VI – DEFINITIONS

15. Definitions used in CNSSI No. 4009, *National Information Assurance Glossary, dated April 2010* (Reference g), apply to this Instruction. Additional and Instruction-specific terms are cited in Annex C.

SECTION VII – REFERENCES

16. The following documents are referenced or provide amplifying or supplementary information. Future updates to referenced documents will be considered applicable to this Instruction.

a. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2012.

b. NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* August 2009 *(includes 2010 errata update).*

c. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.

d. CNSS Directive No. 502, *National Directive on National Security Systems*, December 2004.

e. National Security Directive 42, *National Policy for the Security of National Security Systems*, December 2004.

f. Executive Order 12333, *United States Intelligence Activities*, 4 December 1981, as amended.

g. CNSS Instruction No. 4009, *National Information Assurance (IA) Glossary*, Revised April 2010.

h. Intelligence Community Standard (ICS), Number 500-27, *Collection and Sharing of Audit Data*, 2 June 2011.

i. NIST SP 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, Final Public Draft, February 2013.

ANNEX A – CAPABILITY MATURITY COMPLIANCE MODEL (CMCM)

1. This Instruction provides a phased approach through a Capability Maturity Compliance Model (CMCM) to automate enterprise audit management security control baselines. Compliance with this Instruction must be achieved through the application of the Risk Management Framework found in Committee on National Security Systems (CNSS) Policy No. 2*2, Policy for Information Assurance Risk Management for National Security Systems.*

2. Implementation guidance is organized into a CMCM as shown in Figure 1 below. The approach provides a flexible framework to guide and track the realization of automated Enterprise Audit Management (EAM) as a sequence of successive maturity levels. This approach enables D/As to assess their progress based on their ability to automate EAM security control implementations**.**

	Complexity	**Description**
CMCM Level 1	**Basic**	**Foundational prerequisites**
CMCM Level 2	**Enhanced**	**Partial automation and integration**
CMCM Level 3	**Advanced**	**Complete automation, integration, and dynamic response**

Figure 1 – Capability Maturity Compliance Model (CMCM)

3. D/As must implement all relevant CNSS Instruction (CNSSI) No.1253, *Security Categorization and Control Selection for National Security Systems,* baselines to the satisfaction of the Authorizing Official (AO). When it is not possible to implement a security control via automated means, all CNSSI No. 1253 baseline requirements must still be met manually to the satisfaction of the AO, or a risk-based decision is made to achieve authority to operate (ATO). D/As must develop an implementation plan to the satisfaction of the AO to address the transition from manual to automated security controls where necessary. Automated EAM maturity level compliance is achieved by implementing security controls via automated means (e.g. automated tools, processes, and process support). It is expected that metrics collected for assessing automated EAM progress be consistent with continuous monitoring requirements.

4. Current CNSS policy requires only manual methods of audit management for CNSSI No.1253 Low-Low-Low baselines. National Security Systems (NSS) are operating in an environment of ever-evolving cyber threats. Additional security controls described in this Instruction will be added to all CNSSI No. 1253 baselines to increase the accuracy and speed of cybersecurity incident alerts and provide increased situational awareness on computer networks.

Table 1 – Capability Maturity Compliance Model (CMCM)

EAM CMCM Level 1 (Management)	EAM CMCM Level 1 (Technical)	EAM CMCM Level 2 (Technical)	EAM CMCM Level 3 (Technical)
M1.1	**T1.1**	**T2.1**	**T3.1**
Define roles, responsibilities, and accountability for Security Professionals' (i.e., IAO, IAM, LE/CI) accessible audit accounts (Security Logs) ***AU-1, Audit and Accountability Policy and Procedures***	Implement roles, responsibilities, and accountability for Security Professionals' (i.e., IAO, IAM, LE/CI) accessible audit accounts (Security Logs) ***AU-1, Audit and Accountability Policy and Procedures***	Implement the automated policy to include roles, responsibilities, and accountability for Security Professionals' (i.e., IAO, IAM, LE/CI) accessible audit accounts (Security Logs) ***AU-1, Audit and Accountability Policy and Procedures***	Automate roles, responsibilities, and accountability for Security Professionals' (i.e., IAO, IAM, LE/CI) accessible audit accounts (Security Logs) ***AU-1, Audit and Accountability Policy and Procedures***
M1.2	**T1. 2**	**T2. 2**	**T3. 2**
Establish frequency of policy and procedure reviews/updates ***AU-1, Audit and Accountability Policy and Procedures***	Implement policy and procedure reviews/updates ***AU-1, Audit and Accountability Policy and Procedures***	Automate reviews, updates, and accountability controls ***AU-1, Audit and Accountability Policy and Procedures***	
M1.3	**T1.3**	**T2.3**	**T3.3**
Define audit events that enable audit triggers and alerts to effectively audit the organization. Define thresholds and priorities to support audit triggers and alerts. Note: This is a continuous process influenced by the network/user environment and changing priorities and threats. ***AU-2, Audit Events***	Implement initial organizationally defined audit events that enable audit triggers and alerts to effectively audit the organization. ***AU-2, Audit Events***	Implement additional organizationally defined audit events that enable audit triggers and alerts to effectively audit the organization. ***AU-2, Audit Events***	Implement additional organizationally defined audit events that enable audit triggers and alerts to effectively audit the organization. ***AU-2, Audit Events***

M1.4	T1.4	T2.4	T3.4
Identify procedures to enable or disable audit accounts **AC-2(7)**	Implement procedures to enable or disable audit accounts **AC-2(7)**	Automate procedures to enable or disable audit accounts **AC-2(7)**	
M1.5	**T1.5**	**T2.5**	**T3.5**
Establish the organizationally defined minimum auditable content as part of the record (at a minimum those specified in CNSSI 1253) **AU-3, *AU-3 (1), Content of Audit Records***	Implement sufficient auditable content to be established as part of the record. **AU-3, *AU-3 (1), Content of Audit Records***	Implement capability to dynamically change auditable content to support enterprise analysis of event triggers **AU-3, *AU-3 (1), Content of Audit Records***	Implement automated centralized management of audit record content **AU-3, *AU-3 (2), Content of Audit Records***
M1.6	**T1.6**	**T2.6**	**T3.6**
Define audit data-tagging methodology to enable metadata look-ups of audit content by authorized analysts **AU-3, *AU-3 (1), Content of Audit Records***		Implement audit data-tagging methodology to enable metadata look-ups of audit content by authorized analysts **AU-3, *AU-3 (1), Content of Audit Records***	
M1.7	**T1.7**	**T2.7**	**T3.7**
Define and implement a procedure for alert function in the event of loss-of-audit capability at the device, logger, storage capability, or analyst's desktop ***AU-5, Response to Audit Processing Failures***	Implement procedure for alert function in the event of loss-of-audit capability at the device, logger, storage capability, or analyst's desktop ***AU-5, Response to Audit Processing Failures***	Implement real-time alerting on audit system failures ***AU-5, Response to Audit Processing Failures***	Implement organizationally defined, automated remediation strategies to audit system failures ***AU-5, AU-5(1), Response to Audit Processing Failures***

M1.8	T1.8	T2.8	T3.8
Define event reduction and correlation methodology to support threat determination ***AU-6(3) Audit Review, Analysis and Reporting***	Implement event reduction and correlation at a centralized location ***AU-6(3) Audit Review, Analysis and Reporting***	Implement audit reduction and correlation at an organizationally defined location ***AU-6(3) Audit Review, Analysis and Reporting***	Provide correlated event alerts to a community-defined location ***AU-6(3) Audit Review, Analysis and Reporting***
M1.9	**T1.9**	**T2.9**	**T3.9**
Define how analysts receive and evaluate information to execute response action ***AU-6, Audit Review, Analysis, and Reporting***		Implement automated audit analysis, indication of anomalies, and reporting of unusual activities ***AU-6, Audit Review, Analysis, and Reporting, AU-12 Audit Report Generation***	Implement audit data-monitoring tools for enterprise-wide situational status, event profiles, risk matrix, and dashboards (remediation) ***SI-4(16), Information System Monitoring***
M1.10	**T1.10**	**T2.10**	**T3.10**
Defined organizational reporting frequency ***AU-6, Audit Review, Analysis, and Reporting***	Report findings at organizationally defined frequency ***AU-6, Audit Review, Analysis, and Reporting; AU6(3) Audit Review, Analysis, and Reporting,***	Implement automated audit reporting for events with selectable remediation criteria ***AU-2(3)***,***Auditable Events***; ***AU-6, Audit Review, Analysis, and Reporting; AU-12 Audit Report Generation***	Implement automated audit reporting capabilities to support situational awareness and other organizationally defined defensive activities ***AU-6(3), Audit Review, Analysis, and Reporting***
M1.11	**T1.11**	**T2.11**	**T3.11**
Define audit review approach that generates Security Content Automation Protocol (SCAP)-compliant data supporting		Implement audit review capability that generates SCAP-compliant data supporting automation ***AU-6, Audit Review, Analysis, and***	

automation ***AU-6, Audit Review, Analysis, and Reporting***		***Reporting***	
M1.12	**T1.12**	**T2.12**	**T3.12**
Define authoritative source clock for synchronizing organizational internal IS clocks ***AU-8, Time Stamps***	Implement internal IS clocks synchronized with organizationally defined authoritative source for data collected (e.g.,NTP) ***AU-8(1), Time Stamps***	Implement the IS clock synchronization across organizationally defined systems with authoritative source (e.g.,NTP) ***AU-8(1), Time Stamps***	
M1.13	**T1.13**	**T2.13**	**T3.13**
Define process for ensuring automated back-up of audit data for all devices achieved. ***AU-4, Audit Storage Capacity; AU-9, Protection of Audit Information***	Implement backup of data records on an IS or media separate from the originating source at organizationally defined frequency ***AU-9 Protection of Audit Information***	Automate backup of data records to external system within organizationally defined timeframe, not to exceed one day ***AU-4, Audit Storage Capacity; AU-9 Protection of Audit Information***	Implement an enterprise-wide audit-data back-up storage solution. ***AU-4, Audit Storage Capacity; AU-9 Protection of Audit Information***
M1.14	**T1.14**	**T2.14**	**T3.14**
Define the protection mechanisms for audit data, including frequency, cryptographic process, and accesses consistent with automation goals ***AU-9, Protection of Audit Information***	Implement protection mechanisms to limit access to audit data records (from source or backup) to authorized users ***AU-9, Protection of Audit Information***		
M1.15	**T1.15**	**T2.15**	**T3.15**
Develop a plan for retention of audit data for an organizationally defined period to support investigations	Implement a plan for retention of audit data for an organizationally defined period to support	Implement an automated capability for expiration of retained audit data ***AU-11, Audit Record Retention***	

AU-11, Audit Record Retention	investigations ***AU-11, Audit Record Retention***		
EAM CMCM Level 2 (Management)		**EAM CMCM Level 2 (Technical)**	**EAM CMCM Level 3 (Technical)**
M2.1		**T2.1**	**T3.1**
Define sufficient auditable content to be established as part of the record in support of the use cases ***AU-3 (1), Content of Audit Records***		Capture sufficient auditable content as part of the record in support of the use cases. Implement capability to dynamically change content of auditable events to support enterprise analysis use cases ***AU-3 (1), Content of Audit Records***	

EAM CMCM Level 3 (Management)			EAM CMCM Level 3 (Technical)
M3.1			**T3.1**
Define inter-organizational methodology to report correlated audit alerts of malicious nature to cyber situational awareness authorities for identifying a government response. ***AU-6, Audit Review, Analysis, and Reporting***			Implement inter-organizational methodology to report correlated audit alerts of malicious nature to cyber situational awareness authorities for identifying a government response. ***AU-6, Audit Review, Analysis, and Reporting***

ANNEX B – SET OF AUDITABLE EVENTS

1. D/A must share, where lawful and appropriate, audit data identified below to support Information Assurance, business analytics, personnel security, and other community audit needs related to NSS information resources. This information has been derived from the Intelligence Community Standard (ICS), *Collection and Sharing of Audit Data* (Reference h).

2. Auditable Events or Activities

a. Authentication events

(1) Logons (Success/Failure)

(2) Logoffs (Success)

b. File and Objects events

(1) Create (Success/Failure)

(2) Access (Success/Failure)

(3) Delete (Success/Failure)

(4) Modify (Success/Failure)

(5) Permission Modification (Success/Failure)

(6) Ownership Modification (Success/Failure)

c. Writes/downloads to external devices/media (e.g., A-Drive, CD/DVD devices/printers) (Success/Failure)

d. Uploads from external devices (e.g., CD/DVD drives) (Success/Failure)

e. User and Group Management events

(1) User add, delete, modify, suspend, lock (Success/Failure)

(2) Group/Role add, delete, modify (Success/Failure)

f. Use of Privileged/Special Rights events

(1) Security or audit policy changes (Success/Failure)

(2) Configuration changes (Success/Failure)

g. Admin or root-level access (Success/Failure)

h. Privilege/Role escalation (Success/Failure)

i. Audit and log data accesses (Success/Failure)

j. System reboot, restart and shutdown (Success/Failure)

k. Print to a device (Success/Failure)

l. Print to a file (e.g., pdf format) (Success/Failure)

m. Application (e.g., Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure)

n. Export of information (Success/Failure) include (e.g., to CDRW, thumb drives, or remote systems)

o. Import of information (Success/Failure) include (e.g., from CDRW, thumb drives, or remote systems)

3. Attributable Events Indicating Violations of System/Target (events of concern requiring further analysis or review of additional information.)

a. Malicious code detection

b. Unauthorized local device access

c. Unauthorized executables

d. Unauthorized privileged access

e. After-hours privileged access

f. System reset/reboot

g. Disabling the audit mechanism

h. Downloading to local devices

i. Printing to local devices

j. Uploading from local devices

ANNEX C – DEFINITIONS

1. Definitions used in CNSSI No. 4009, *National Information Assurance Glossary*, revised April 2010 (Reference g), apply to this Instruction. Below is an additional term and its definition. Within this Instruction these definitions are used exclusively for these terms. [These terms are proposed for inclusion in the next version of CNSSI No. 4009.]

Enterprise Audit Management Capability:

Involves the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of the capability. An Enterprise Audit Management solution should be deployed to collect, store, and provide access to audit data. For each type of audit (specific to system/mission/data), auditable events are identified, auditing is conducted to properly capture and store that data, and analysis and reporting are performed. Certain high-profile events should trigger automated notification to designated individuals, such as system security officers or D/As incident response center/team.