INTELLIGENCE COMMUNITY STANDARD NUMBER 500-27

(U) COLLECTION AND SHARING OF AUDIT DATA (EFFECTIVE: 2 JUNE 2011)

A. (U) AUTHORITY: The National Security Act of 1947, as amended; Executive Order 12333, as amended; Intelligence Community Directive (ICD) 101, *Intelligence Community Policy System*; ICD 500, *Director of National Intelligence Chief Information Officer*; ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*; ICD 502, *Integrated Defense of the Intelligence Community Information Environment*; ICD 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation;* and other applicable provisions of law.

B. (U) PURPOSE

1. (U//~~FOUO~~) Intelligence Community (IC) elements shall audit information resources within the IC information environment (hereafter referred to as IC information resources) to protect national intelligence, identify threats (including insider threats), detect and deter penetration of IC information resources, reveal misuse, identify usage trends and for other lawful purposes. This Standard provides guidance for implementing uniform information security requirements and procedures, as established by ICD 500.

2. (U//~~FOUO~~) Audit data shall be collected on IC information resources for the purposes outlined above and shall be shared with each respective user's gaining and employing IC element, or department or agency as appropriate, to include both contractors and government personnel.

3. (U//~~FOUO~~) This Standard provides for the collection and sharing of audit data to support counterintelligence (CI), information assurance (IA), business analytics (BA), personnel security (PS), and other community audit needs related to IC information resources.

4. (U//~~FOUO~~) The collection and sharing of audit data will:

a. (U//~~FOUO~~) Enable IC elements to identify and evaluate anomalous activity involving IC information resources.

b. (U//~~FOUO~~) Enable IC elements to identify and assess misuse (intentional or inadvertent), and/or exploitation of IC information resources, whether the source is external or internal.

c. (U//~~FOUO~~) Support authorized investigations, oversight, and inquiries.

d. (U//~~FOUO~~) Deter unauthorized use of IC information resources.

e. (U//~~FOUO~~) Enable IC elements to assess the effectiveness of intelligence information sharing.

C. (U) APPLICABILITY

1. (U) This Standard applies to the IC, as defined by the National Security Act of 1947, as amended, and such other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

D. (U) IMPLEMENTATION

1. (U//~~FOUO~~) The requirements of this Standard shall be implemented on all IC information resources, consistent with the risk management approach prescribed in ICD 503. Requests for waivers to this requirement shall be submitted in accordance with IC Standard (ICS) 500-20, *Intelligence Community Enterprise Standards Compliance*. IC elements are to provide to the IC Chief Information Officer (IC CIO) an implementation plan for the requirements set forth in this Standard within 60 days of signature.

2. (U//~~FOUO~~) The events and activities identified in Appendix B of this Standard shall be collected on IC information resources. The IC CIO shall promulgate IC enterprise standards with details for collecting these auditable events consistent with ICS 500-20. IC information resources shall have the ability to collect such audit data through automated means and store the information securely. The information will be marked and handled at the appropriate classification and sensitivity levels.

3. (U//~~FOUO~~) IC elements shall share, where lawful and appropriate, audit data identified in Appendix B of this Standard to support CI, IA, BA, PS, and other community audit needs related to IC information resources. This sharing shall be consistent with access restrictions developed pursuant to Section D.6 of this Standard. IC elements are to use IC enterprise standard, *IC Enterprise Audit Exchange Technical Specification* (AUDIT.XML) to guide near-term sharing. To standardize the sharing of audit data, the IC CIO shall promulgate an enterprise audit framework that will drive the development of additional IC enterprise standards and identify how the IC shall share audit information consistent with Section D.6. Within 60 days of promulgating the enterprise audit framework, IC elements are to provide to the IC CIO an updated implementation plan that includes requirements outlined in the enterprise audit framework.

4. (U//~~FOUO~~) IC information resources shall have the capability to collect key strokes and full application content (email, chat, imports, exports, etc.), obtain screen captures, and perform file shadowing for all lawful purposes, to include detecting unauthorized use or disclosure.

a. (U) This capability shall be used only in accordance with applicable law, policy, and regulations.

b. (U//~~FOUO~~) IC elements shall develop internal processes and procedures for using these specific capabilities and the information collected, in consultation with their respective legal counsel and civil liberties and privacy officials.

5. (U//~~FOUO~~) IC information resources shall display a standard banner to be promulgated by the IC CIO, that provides notice of, and obtains user consent to, the collection and monitoring of all user activities. This standard banner shall be implemented in coordination with legal counsel, as well as with civil liberties and privacy officials, to ensure legal, civil rights, civil liberties, and privacy issues are appropriately addressed.

6. (U//~~FOUO~~) Audit data shall be safeguarded, in accordance with applicable law, policy, and department or agency regulations, at rest, in transit, and during presentation, to include appropriate limitations on access and use. Audit data shall be protected from unauthorized access, modification, or destruction and shall be reviewed at least weekly for action by the IC element.

7. (U//~~FOUO~~) IC elements shall develop procedures for accessing audit data. Each IC element shall ensure that access to audit data is restricted to personnel who require the information to perform their authorized functions. Personnel authorized to access data shall be trained regarding all applicable laws and policies and the consequences of misuse of audit data.

8. (U//~~FOUO~~) IC elements shall implement this Standard consistent with ICS 500-20.

9. (U) Audit data shall be retained in accordance with the applicable records control schedule.

10. (U) Guidance supporting insider threat detection is provided in ICS 700-2, *Use of Audit Data for Insider Threat Detection.*

E. (U) RESPONSIBILITIES

1. (U) IC elements shall:

a. (U//~~FOUO~~) Collect audit data pertaining to IC information resources pursuant to the requirements of this Standard and in accordance with ICS 500-20.

b. (U//~~FOUO~~) Ensure audit data is attributable to a unique user and/or IC information resource. To the extent that audit data attributable to a unique user may be shared with others, such sharing shall be limited to the least amount required to assess the threat or to address the concern for which the sharing is requested.

c. (U) Ensure that adequate security and privacy controls are implemented to protect the data, including oversight of compliance by audit personnel and monitoring of audit personnel activities. Ensure that personnel authorized to access audit data shall be trained regarding applicable laws and policies and the consequences of misuse of audit data.

d. (U//~~FOUO~~) Submit to the IC CIO any request for a waiver to the requirements herein in accordance with ICS 500-20. Waiver requests with regard to the requirements of this Standard shall be approved by the IC CIO in consultation with the National Counterintelligence Executive (NCIX).

e. (U//~~FOUO~~) Share, as appropriate and consistent with applicable law, information regarding audit events pertaining to users and processes acting on behalf of a user accessing an IC information resource with each respective user's gaining or employing IC element, or department or agency. To enable this sharing, each IC element shall have the capability to receive and store audit data securely and in accordance with the requirements of this Standard. Additionally, each IC element shall determine if the collection and use of such data requires a Privacy Act System of Records Notice (SORN).

f. (U//~~FOUO~~) Share audit data regarding detected anomalies on IC information resources that potentially stem from an insider threat in a timely manner with all appropriate organizations responsible for insider threat detection (which may include the user's gaining or employing IC element, or department or agency).

g. (U//~~FOUO~~) Provide an implementation plan consistent with Section D.

h. (U) Maintain the record copy of the audit data collected pursuant to the Federal Records Act and in accordance with the IC element's applicable records control schedules.

i. (U) Provide quarterly reports to the IC CIO on the extent to which the requirements of this Standard are implemented on IC information resources. Such reporting shall be presented to the IC CIO and begin October 1, 2011.

j. (U) Ensure that notice of any unauthorized access, use or sharing of audit data containing personally identifiable information is handled consistent with applicable data breach notification policies.

2. (U) The IC CIO shall:

a. (U) Develop specific audit-related guidance necessary for addressing IC audit needs associated with IC information resources, to include guidance related to Section D.3. Such guidance shall be developed in consultation with the Office of General Counsel and the Civil Liberties Protection Officer to ensure privacy and civil liberties considerations are addressed.[1]

b. (U) Promulgate IC enterprise standards consistent with requirements pursuant to the governance process in ICS 500-20. Requirements for the development of IC enterprise standards for audit events to support insider threat detection shall be developed and promulgated in consultation with the NCIX.

[1] 50 U.S.C. 403-3d

c. (U) Evaluate and monitor the implementation of this Standard at least annually.

d. (U) In support of insider threat detection, notify the NCIX of:

(1) Non-compliance by the IC elements with this Standard or associated IC enterprise standards, and share with NCIX the IC elements' plans of action and milestones to address non-compliance.

(2) Waiver requests submitted in accordance with Section E.1.d of this Standard.

F. (U) EFFECTIVE DATE: This Standard becomes effective on the date of signature.

2 June 2011

Al Tarasiuk
Assistant Director of National Intelligence and
Intelligence Community Chief Information Officer

Date

(U) Appendix A - Terms and Definitions

(U) Audit: Provides authorized personnel with the ability to review and examine any action that can potentially cause access to, generation of, or affect the release of classified or sensitive information.

(U) Employing element: The IC element from which an employee on a joint IC duty rotational assignment is detailed. The detailed employee's permanent position of record remains with the employing element, and the detailed employee remains on the permanent rolls of that employing element during the joint IC duty rotational assignment, unless other administrative arrangements are agreed to by the employing and gaining element (ICD 601, *Joint IC Duty Assignments*, 4 September 2009).

(U) File shadowing: The replication of data to another location in a systematic way that produces an identical copy of that data. The location can be as nearby as another disk in the same server, or in another server or workstation in a completely different geographic location.

(U) Gaining element: The IC element to which an employee is detailed while on a joint IC duty rotational assignment (ICD 601, *Joint IC Duty Assignments*, 4 September 2009).

(U) Information resources: Information and related resources, such as personnel, equipment, funds, and information technology (IC Policy Guidance (ICPG) 500.2, *Attribute-Based Authorization and Access Management*, 23 November 2010).

(U) Insider threat: The threat that an insider will use authorized access to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities.

(U) Intelligence Community Information Environment: The IC information environment is defined as the individuals, organizations, and Information Technology capabilities that collect, process, or share Sensitive Compartmented Information, or that regardless of classification, are operated by the IC and are wholly or majority National Intelligence Program-funded (e.g., DNI-U). The IC information environment is an interconnected shared risk environment where the risk accepted by one IC element is effectively accepted by all (ICD 502, *Integrated Defense of the Intelligence Community Information Environment*, 11 March 2011).

(U) Appendix B - Set of Auditable Events

I. (U) Auditable Events or Activities

- Authentication events
    - Logons (Success/Failure)
    - Logoffs (Success)
- File & Object events
    - Create (Success/Failure)
    - Access (Success/Failure)
    - Delete (Success/Failure)
    - Modify (Success/Failure)
    - Permission Modifications (Success/Failure)
    - Ownership Modifications (Success/Failure)
- Writes/downloads to external devices/media (e.g., A-Drive, CD/DVD drives, printers) (Success/Failure)
- Uploads from external devices/media (e.g., CD/DVD drives) (Success/Failure)
- User & Group Management events
    - User add, delete, modify, suspend, lock (Success/Failure)
    - Group/Role add, delete, modify (Success/Failure)
- Use of Privileged/Special Rights events
    - Security or audit policy changes (Success/Failure)
    - Configuration changes (Success/Failure)
- Admin or root-level access (Success/Failure)
- Privilegc/Role escalation (Success/Failure)
- Audit and log data accesses (Success/Failure)
- System Reboot, Restart & Shutdown (Success/Failure)
- Print to a device (Success/Failure)
- Print to a filc (e.g., pdf format) (Success/Failure)
- Application (e.g., Netscape, IE, Lotus Notes, etc.) initialization (Success/Failure)
- Export of information (Success/Failure)
- Import of information (Success/Failure)

II. (U) Auditable Event Details/Information Elements

- Date and time of the event using the common network time (e.g., Network Time Protocol).

- Type of the event (e.g., login, print, etc.)
- Identifier indicating the source/system of the event activity.
- Identifier indicating the identity of the subject or actor (e.g., UserId, ProcessId, etc.
- Details identifying any objects or resources accessed or involved (aka Resource List), e.g., files (including location), document id, peripherals, storage devices, etc.
- Outcome (e.g., Success or Failure).

III. (U) Attributable Events* Indicating Violation of System/Target

- Malicious code detection
- Unauthorized local device access
- Unauthorized executables
- Unauthorized privileged access
- After-hours privileged access
- System reset/reboot
- Disabling of the audit mechanism
- Downloading to local devices
- Printing to local devices
- Uploading from local devices

* "Events" of concern that require further analysis or review of additional information or events. Some of these may require tools or utilities (e.g., malicious code detection).