NATIONAL INSIDER THREAT TASK FORCE (NITTF)
Office of the Co-Directors
Washington, DC 20511

NITTF-2014-008

MEMORANDUM FOR: Senior Insider Threat Program Official
All Executive Branch Departments and Agencies

SUBJECT: Clarification of Enterprise Audit Management (EAM), User Activity Monitoring (UAM), Continuous Monitoring, and Continuous Evaluation

1. Consistent with the recently approved Committee on National Security Systems (CNSS) Directive No. 504, CNSS Instruction 1015, and CNSS Instruction No. 4009, this memorandum reiterates the definitions of Enterprise Audit Management, User Activity Monitoring, and Continuous Monitoring, which are related activities that seek to identify anomalous behavioral and network events indicative of a potential compromise. Additionally, the memorandum clarifies the connection between Insider Threat programs and the nascent Continuous Evaluation Program to enhance personnel security.

2. On 21 November 2012, the President of the United States issued the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* requiring each Executive Branch department and agency (D/A) with access to classified material to establish an insider threat program. Insider Threat programs include the capability to monitor user activity on networks and manually and/or electronically gather, integrate, review, assess and respond to information derived from several sources, including Counterintelligence and Security, Information Assurance, and Human Resources.

3. The following definitions are published in, or are being added to the next update of, *Committee on National Security Systems (CNSS) Instruction No. 4009, National Information Assurance Glossary.*

    a. **Enterprise Audit Management** – CNSS Instruction No. 1015, Enterprise Audit Management (EAM) Instruction for National Security Systems defines EAM as "the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of this 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 trigger automated notification to designated individuals, such as system security officers or D/As incident response center/team."

CNSSI No. 1015 also states that EAM, "...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. 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."

b. **User Activity Monitoring** – CNSS Directive No. 504, Directive on Protecting National Security Systems from Insider Threat, defines User Activity Monitoring (UAM) as "the technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and to support authorized investigations." Annex B also states, "Each D/A must have the following minimum capabilities to collect user activity data: key stroke monitoring and full application content (e.g., email, chat, data import, data export), obtain screen captures, and perform file shadowing for all lawful purposes. UAM data must be attributable to a specific user. The D/A should incorporate this data into an analysis system capable of identifying anomalous behavior..."

c. **Continuous Monitoring** – CNSS Instruction No. 4009 defines Continuous Monitoring as "the process implemented to maintain a current security status for one or more information systems or the entire suite of information systems on which the operational mission of the enterprise depends. The process includes *but is not limited to*:

i. The development of a strategy to regularly evaluate selected Information Assurance (IA) controls/metrics;
ii. Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events;
iii. Recording changes to IA controls, or changes that affect IA risks, and;
iv. Publishing the current security status to enable information sharing decisions involving the enterprise. "

4. The following summaries highlight the similarities and differences between EAM, UAM and Continuous Monitoring.

a. EAM is a structured, consistent and continuous collection and reporting process across the whole of an organization for identifying, assessing, deciding upon responses to, and reporting upon the efficiencies of, or upon threats that affect the operational continuance of functionality. EAM is not intended to, nor does it collect, report, or otherwise act upon specific analysis of employee threat behaviors.

b. UAM is a structured, consistent and continuous collection and reporting process across the whole of an organization at the device level for identifying, assessing, deciding upon responses to, and acting upon specific analysis of employee threat behaviors. Unlike EAM, the purpose of UAM is to gather detailed and substantive content about behavioral activity, which may be indicative of an insider threat.

c. Continuous monitoring is one of six steps in the Risk Management Framework (RMF) described in NIST Special Publication 800-37, Revision 1, Applying the Risk Management Framework to Federal Information Systems (February 2010). The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation (including threat space).

The three capabilities, EAM, UAM, and Continuous Monitoring, contribute to overall system security and insider threat detection.

5. **Continuous Evaluation (CE)** is a key component of Insider Threat programs. Executive Orders 12968 and 13467 authorize continuous evaluation of individuals determined eligible for access to classified information. As defined in E.O. 13467, CE means reviewing the background of an individual who has been determined eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information. As currently planned, CE will look at investigative elements deemed most productive for evaluating an individual's continuing eligibility to access classified information on a more frequent or continuous basis than the current investigation periods. When information on a cleared individual meets a threshold of concern as a result of these database checks, the employing or sponsoring agency will be responsible for reviewing the information and determining appropriate action, such as referring the matter to an adjudicator, conducting additional investigation, providing the information to the agency's Insider Threat program, or referring the subject to a counterintelligence component, just as occurs with any other investigation.

If you have any questions, please contact the undersigned or the NITTF at NITTFAsistance@dni.gov (or NITTF-Assistance@dni.ic.gov).

Patricia L. Larsen 3/14/2014

Patricia L. Larsen
Co-Director
National Insider Threat Task Force