

June
2023



INSIDER THREAT INDICATORS IN USER ACTIVITY MONITORING

JOB AID

INTRODUCTION

Logging, monitoring, and auditing of information system activities can lead to early discovery and mitigation of behavior indicative of insider threat. Insider Threat policies require User Activity Monitoring (UAM) on classified networks in support of Insider Threat Programs for:

- DOD Components under DODD 5205.16
- Federal Agencies under E.O. 13587 and National Minimum Standards
- Cleared Industry under the 32 CFR Part 117 or NISPOM Rule

Implementation will be specific to your location, but all organizations must:





- Define what will be monitored
- Indicate how monitoring will be instituted
- Inform users of monitoring actions via banners
- Identify indicators that require review (e.g., trigger words, activities)
- Protect user activity monitoring methods and results
- Develop a process for verification and review of potential issues
- Establish referral and reporting procedures

UAM also plays a key role in insider threat programs. As such UAM development should include consideration of potential acts of violence against organizational resources, including suicidal ideation.

Click on the links below for more information on developing your program.

UAM Policy and Implementation	Defining Activity Monitoring	Key Word Indicators and Triggers	UAM Log Review Process	Reporting and Referral Procedures
---	--	--	--	---

Below are some of the areas to consider when you are developing UAM indicators and triggers for monitoring and reporting. The illustrations below depict some of the potential risk indicators that may be detected by UAM.

 Access Attributes	 Foreign Influence and Preference	 Financial Considerations	 Reporting Insider Threat Indicators is required under Executive Order 13587, DOD Directive 5205.16 and the National Industrial Security Program.
 Personal Conduct	 Substance Abuse and Alcohol Consumption	 Criminal Conduct	



For more Insider Threat resources visit:

<https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/>

UAM POLICY AND IMPLEMENTATION

Governance, or the policies and procedures you enact for your Insider Threat Program, will guide your efforts in monitoring user activities on your organization's classified networks. These efforts should include user and group management, use of privileged and special rights, and security and policy changes. Key components of governance include having employees sign agreements acknowledging monitoring and implementing banners informing users that their system and network activity is being monitored. Monitoring these elements ensures that users' access is limited to what is essential for their role. This allows you to then prioritize monitoring efforts. It also allows you to identify users who are abusing their privileges.

User Activity Monitoring helps identify users who are abusing their access and may be potential Insider Threats. This includes monitoring file activities, such as downloads, print activities (such as files printed), and search activities. Monitoring these activities can identify abnormal user behaviors that may indicate a potential Insider Threat. While you cannot monitor every aspect of these activities, you can prioritize efforts as they relate to the systems and information that require the most protection.

System Activity Monitoring will allow your program to identify possible system misuse. Activities or events to monitor include logons and logoffs, system restarts and shutdowns, and root level access.



Monitoring these activities identifies when the network is being accessed, any potential software installs, and whether someone is accessing or making changes to the root directory of a system or network.

Any UAM Program should, at minimum, be implemented with Chief Information Officer concurrence before, during, and after a UAM system is considered.



References:

- Industry
- DOD
- Federal Agencies

DEFINING ACTIVITY MONITORING

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

The following definitions are published in the Committee on National Security Systems (CNSS) Instruction No. 4009, National Information Assurance Glossary.

User Activity Monitoring (UAM)- 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 investigations.

Enterprise Audit Management (EAM)- The identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of this capacity. A EAM solution should be deployed to collect, store, and provide access to audit data.

Continuous Monitoring- 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.

Continuous Vetting (CV)- Continuous Vetting (CV) is a process that involves regularly reviewing a cleared individual's background to ensure they continue to meet security clearance requirements and should continue to hold positions of trust.

CV works as automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility. When DCSA receives an alert, it assesses whether the alert is valid and worthy of further investigation. DCSA investigators and adjudicators then gather facts and make clearance determinations. CV helps DCSA mitigate

personnel security situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances.

Trusted Workforce 2.0, the whole-of-government approach to reform the personnel security process and establish a single vetting system for the U.S. Government, began implementation in 2018 following extensive planning and inter-agency coordination.

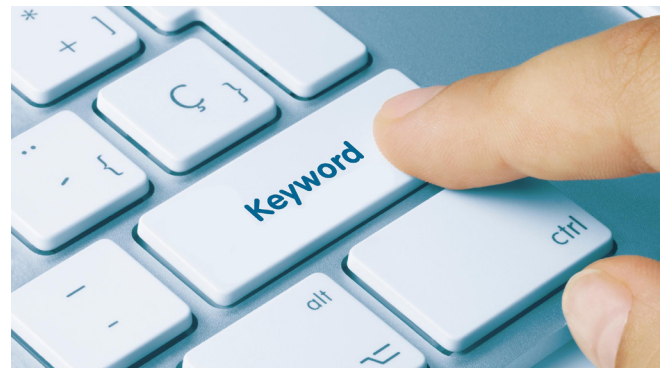
Relevant insider threat information partially realizes the agency specific information required for each CV program. While complementary, insider threat programs operating with robust UAM are not a requirement.

KEY WORD INDICATORS AND TRIGGERS

Organizations monitoring for theft of classified and/or confidential information need to consider the wide variety of ways that information is pilfered and customize their detection strategy accordingly following unique patterns of insider threat behavior (i.e. intellectual property (IP) theft, IT sabotage, fraud, espionage, and accidental insider threats).

Every organization has a unique network topology whose characteristics, such as bandwidth utilization, usage patterns, and protocols, can be monitored for security events and anomaly detection. Deviations from normal network behavior can signal possible security incidents, including insider threats. However, administrators must have visibility into a network to understand it. Various tools and software packages can collect information about keyword activity behavior and develop a network topology. Additionally, organizations should consider that the use of keywords and triggers are dynamic to the current threats and policies which are subject to change over time.

Several tools are available that enable the organization to perform functions like alerting administrators to emails with unusually large attachments; tagging documents that should not be permitted to leave the network; tracking or preventing printing, copying, or downloading of certain information, such as personally identifiable information or documents containing certain words like new product codenames; tracking of all



documents copied to removable media; preventing or detecting emails to competitors, outside the U.S., to Gmail or Hotmail accounts, and so on.

Organizations may find it challenging to maintain employee privacy while collecting data to establish a baseline. The collection, use, maintenance, and dissemination of information critical to the success of government efforts to counter insider threats must comply with all applicable laws and policy issuances, including those regarding whistleblower, civil liberties, and privacy protections.



Additional Resources:

Carnegie Mellon Insider Threat Best Practices
OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

UAM LOG REVIEW PROCESS

Security and logging capabilities have reached the point where data overload is as challenging a problem as data collection. Information security vendors have responded to the expanding cyber threat landscape with a plethora of security solutions. This growth has introduced two major challenges to the problem of cybersecurity: volume and complexity. To overcome the barriers of volume and complexity, organizations must identify exactly which of their data feeds are critical. Use a log correlation engine to log, monitor, and audit employee actions. Successful implementation of such a solution depends on knowing what data to collect. Simply logging all online events is not sufficient to protect an organization's infrastructure from malicious activity. Correlating events will produce more relevant alerts and better informed decisions.

Audit policy for US Government systems is established in the [Federal Information Security Management Act \(FISMA\)](#). This policy is reinforced for DOD Components under both Cybersecurity and Insider Threat policy and for cleared industry under the NISPOM.

Audit logs are an important part of continuous monitoring and fundamental to operational resilience. As stated in DODI 8500.01, Cybersecurity policy on operational resilience, "Attempts made to reconfigure, self-defend, and recover should produce an incident audit trail." DODD 5205.16, The DOD Insider Threat Program, states that Component programs will maintain an "...integrated capability to monitor and audit information for insider threat detection and mitigation..."

[Part 117.18](#) of 32 CFR or the NISPOM Rule, addresses the Information Systems Security and cites that The CSA will issue guidance based on requirements for federal systems, pursuant to 44 U.S.C. Ch. 35 of subchapter II, also known as the "Federal Information Security Modernization Act," and as set forth in National Institute of Standards and Technology (NIST) Special Publication 800–37.

The primary purpose of audits is to promote User accountability. While requirements may be different depending on your organization, the following are recommended as a good baseline: conduct Audit Log Reviews weekly and archive Audit Logs for a period of one year or one review cycle. Applicable laws, regulations, and policies may mandate a different period of retention.

For more information, see the "Continuous Monitoring" eLearning course available at [CDSE.edu](#).



Additional Resources:

OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources"

REPORTING AND REFERRAL PROCESS

Insider Threat Programs must report certain types of information. DOD, Federal agency, and industry Insider Threat Programs operate under different regulations and requirements for reporting.

Federal Insider Threat Programs, including those in DOD, are obligated to report to the FBI under Section 811 of the Intelligence Authorization Act when classified information is being, or may have been,

disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. In addition, Federal Insider Threat Programs must follow any other internal reporting procedures established within the organization. To report to the FBI, use the [FBI Headquarters email point of contact](#) for secure reporting or contact your local field office.

DOD Components are also required to report information that meets identified thresholds to the Defense Insider Threat Management and Analysis Center via the DITMAC System of Systems or DSOS. In addition, items meeting reporting thresholds under the DODD 5240.06, Counterintelligence Awareness and Reporting, must be reported to the cognizant Counterintelligence Office.

Under 32 CFR Part 117.8 (b) or NISPOM Rule, industry must report certain events that may have an effect on the status of the entity's or an employee's eligibility for access to classified information. These include events that indicate an insider threat to classified information or to employees with access to classified information, as well as events that affect the proper safeguarding of classified information or that classified information has been, or suspected to be lost or compromised.

Under certain circumstances, such as the opening of an investigation or inquiry, your Program may need to cease activities upon referral. In other instances,



the Program may be able to employ alternate mitigation options concurrent with external actions. Your Insider Threat Program must ensure that early actions taken in incident response do not interfere with the ability of law enforcement or counterintelligence to conduct investigations or operations, or inhibit future prosecution, in cases that require reporting to external agencies. Work with your general counsel and the referral agency to ensure that any evidence associated with the incident is handled properly and adheres to the proper chain of custody. See the

CDSE eLearning courses [Preserving Investigative and Operational Viability in Insider Threat](#) and [Insider Threat Mitigation Response](#) for more information.



Additional Resources:

Insider Threat Toolkit: Reporting Tab

PRIVACY & CIVIL LIBERTIES

Although lawful agency monitoring of employee communications serves legitimate purposes, federal law also protects the ability of workers to exercise their constitutional rights including the right to report questionable government activity without fear of retaliation. The collection, use, maintenance, and dissemination of information critical to the success of government and industry efforts to counter insider threats must comply with all applicable laws and policies, including those regarding whistleblower, civil liberties, and privacy protections. Laws, policies, and regulations vary depending on your organization.

Federal agencies, including the DOD, must protect Personally identifiable information (PII) for U.S. persons in accordance with section 552a of Title 5, U.S.C. (also known as "The Privacy Act of 1974") and other federal regulations. In addition, all Constitutional rights must be protected. Activities related to the DOD insider threat program, including information sharing and collection, must comply with



DOD Privacy policy and Civil Liberties Policies. Cleared industry programs are also required to comply with applicable federal, state, and local privacy and civil liberties policies and regulations.

One way to balance information-sharing and privacy is to minimize the number of personnel who have access to sensitive data. While all information owners (i.e. human capital, corporate or agency records

custodians, supervisors and non-management workers, security groups, etc.) may contribute their threat detection data and ideas, only a small, core insider threat team should receive and analyze that information. These inputs may be the result of a data call, or they may be a real-time, automated data feed. Each stakeholder should have a trusted agent who can provide data feeds or additional information. The insider threat team should identify trusted agents ahead of time, so they can be contacted immediately when an incident occurs.

Organizations should **consult legal counsel before implementing any monitoring program** to ensure

they meet all legal requirements and disclosures. Moreover, organizations should evaluate their monitoring policies and practices, and take measures to ensure that these policies and practices do not interfere with lawfully disclosing questionable government activity.



REFERENCES

INDUSTRY REFERENCES

- 32 CFR Part 117 (NISPOM Rule)
- DCSA Assessment and Authorization Process Manual, 31 Aug 2020

DOD REFERENCES

- Department of Defense Directive 5205.16 - The DOD Insider Threat Program
- DOD 5400.11, Ch. 1, "DOD Privacy and Civil Liberties Programs" December 8, 2020
- DOD 6025.18-R, DOD Health Information Privacy Regulation, March 13, 2019
- DOD Directive 5143.01, "Under Secretary of Defense for Intelligence," April 6, 2020
- DOD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- DOD Instruction 1000.29, Ch. 1, "DOD Civil Liberties Program," November 26, 2014
- DOD Instruction 8580.02, "Security of Individually Identifiable Health Information in DOD Health Care Programs," August 12, 2015
- DOD Manual 5240.01, Ch. 3, "Procedures Governing the Conduct of DOD Intelligence Activities," November 9, 2020
- DOD Manual 8910.01, Volume 1, Ch. 4, "DOD Information Collections Manual: Procedures for

DOD Internal Information Collections," December 5, 2022

- Secretary of Defense Memorandum, "Final Recommendations of the Washington Navy Yard Shooting Internal and Independent Reviews," March 18, 2014
- DODD 5205.83, "DOD Insider Threat Management and Analysis Center (DITMAC)" March 30, 2017

FEDERAL AGENCY REFERENCES

- Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
- Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Dated Nov. 21, 2012)
- United States Code, Title 5, Section 522a (also known as "The Privacy Act of 1974")
- GAO- Federal Information System Control Audit Manual
- NIST- Federal Information System Management Act
- U.S. Office of Special Counsel Agency Monitoring Policies and Whistleblower Disclosures Memo Feb 01, 2018