MONITOR CLASSIFIED NETWORK ACTIVITY

NISPOM Chapter 8 provides the minimum requirements for management, operational and technical controls, and the DSS Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM Change 2, Version 3.3 May 2016 incorporates minimum standards for contractors' Insider Threat Programs as they relate to information systems. The Insider Threat program requirements only affect monitoring network activity on CLASSIFIED systems; there is no requirement to monitor unclassified networks.

Requirements:

- **Monitor the classified network**
- **Protect the methods and information associated with monitoring**
- **Signed user agreements**
- **Login banners**

Contractors will monitor and review user activity to detect Insider Threat activity and protect the methods used and information obtained. The DSS ODAA Process Manual provides specific guidance for the auditing and monitoring of contractor classified information systems under User Activity Monitoring/Auditing (6.7.1).

Additional Requirements

- User Training (4.1.1): All classified IS users will be trained on their responsibilities and the training will include information related to the Insider Threat Program.
- Use of System Logon Banners (6.2): Classified IS users will be notified at logon that their activity is subject to monitoring.
- Separation of Function (6.1.1): For PL-3 systems, the Information System Security Manager (ISSM) will ensure the functions of the Information System Security Officer (ISSO) and the system manager will not be performed by the same person.

Getting Started:

- Governance, or the policies and procedures you enact for your Insider Threat Program, will guide your efforts in monitoring user activity on your organization's classified networks. These 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 components 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.
- 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.
- 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.
- Key Elements to your program will include Monitoring Considerations, Integration, Audit Requirements, Analysis, and Gather. Click each item to learn more.

Best Practices:

- The ISSM plays an important role in the contractor's Insider Threat Program and reports information system activities related to the program to the contractor's Insider Threat Senior Official (ITSO).
- Monitoring activity on classified networks is essential to the success of your Insider Threat Program.
- Successful monitoring will involve several levels of activities.
- Once policies are in place, system activities, including network and computer system access, must also be considered and monitored.
- Consider enforcing the principle of least privilege to facilitate limitations on access and the monitor and review of inconsistent access or privilege elevation.

- Finally, an Insider Threat Program must also monitor user interactions on the classified networks and information systems.

Related Training and Resources:

- **eLearning Course: Continuous Monitoring Course**
- **Insider Threat Toolkit Tab: Cyber Insider Threat**