FORCEPOINT
POWERED BY Raytheon

Need to establish an Insider Threat program to meet NISPOM Change Order 2 requirements?

In May, the Department of Defense issued a mandate that contractors and the Defense Industrial Base (DIB) with access to classified information establish an Insider Threat program. Contractors must have a ***written plan*** to begin implementing insider threat requirements by **November 30, 2016**. This includes the appointment of an Insider Threat Program Senior Official (ITPSO).

This requirement can be found in Change 2 to DoD 5220.22-M, "National Industrial Security Operating Manual (NISPOM)," published May 18, 2016.

Forcepoint™ has been trusted by the US Government and Fortune 500 companies for more than 15 years to provide compliance with user activity monitoring (UAM) directives. Forcepoint's SureView® Insider Threat is uniquely suited to support customers in complying with NISPOM Change Order 2.

Minimum NISPOM Change Order 2 Requirements Checklist

Contractors must establish and maintain an insider threat program to gather, integrate and report information indicative of a potential or actual insider threat:

NISPOM CHANGE 2 REQUIREMENT	FORCEPOINT SUREVIEW INSIDER THREAT
Capability to gather relevant insider threat information across the contractor facility (1-202a)	✓ Convergence, a SureView Insider Threat API, aggregates data from external sources.
Access, share, compile, identify, collaborate across the organization (cleared), report relevant information covered by the 13 personnel security adjudicative guidelines (1-202a)	✓ Convergence brings in data such as DLP alerts and HR data (name, job title, performance reviews, etc.) to provide additional context.
Deter cleared employees from becoming insider threats (1-202a)	✓ Building an Insider Threat program with SureView Insider Threat at the center provides a starting point for organizations to develop policies and practices they can use to detect and deter "risky" behavior.
Detect insiders who pose a risk to classified information (1-202a)	✓ SureView Insider Threat deploys user-centric, policy-based methodologies that proactively detect risks to classified information.
Mitigate risk of an insider threat (1-202a)	✓ SureView Insider Threat provides context surrounding an event or action, enabling company policies to be re-enforced in an effective and responsible manner.
Certify annually to DSS in writing that a self-inspection has been completed according to provisions in NISPOM paragraph 1-207b	✓ As part of a complete Insider Threat program, SureView Insider Threat provides necessary supporting data and built-in reporting capabilities.

NISPOM CHANGE 2 REQUIREMENT	FORCEPOINT SUREVIEW INSIDER THREAT
Contractors must report relevant and credible information regarding cleared employees; information of potential or actual insider threat covered by any of 13 personnel security adjudicative guidelines (1-300)	✓ SureView Insider Threat contains built-in reports, including one that identifies top users by their policy violations. Custom reports can be created as needed, and SureView Insider Threat can compile the data into a case file that can be exported for use in external sources.
User activity monitoring on classified information systems (FISMA, NIST, CNSS) (8-100d)	✓ SureView Insider Threat is compliant with all UAM requirements.
Keystroke Monitoring	✓ SureView Insider Threat monitors and captures all keystrokes and the text resulting from those keystrokes. Custom policies mask capturing passwords or credit card numbers.
Application Monitoring	✓ SureView Insider Threat monitors applications at the endpoint and in the Cloud (through integration with Forcepoint's TRITON® suite).
Video Capture and Playback: Windows & Mac	✓ SureView Insider Threat provides the best-in-class, continuous video capture across multiple screens. Captures user activity before, during and after an event trigger.
File Shadowing (i.e., collecting a copy of the file)	✓ SureView Insider Threat collects Office documents and other files, PDFs, presentations, spreadsheets, database files, formatted text, CAD, Image, .exe, archive, multimedia, etc.

Why SureView Insider Threat?

SureView Insider Threat provides you with the forensic evidence needed for undeniable attribution and chain of custody to simplify investigations, prosecution and to demonstrate compliance.

Proactive, policy-based user behavior monitoring acts as an early warning indicator to identify suspicious behavior, whether malicious or accidental. SureView Insider Threat provides the visibility and context required to rapidly mitigate risky user behavior. It also integrates with data sources, such as Forcepoint's DLP solution, for a holistic approach that meets the most challenging compliance requirements.

SureView Insider Threat delivers unrivaled visibility into computer users' early activity, helping you to stop data theft and loss by:

- **DETECTING** suspicious activity, whether malicious or accidental.
- **PREVENTING** a hijacked system, a rogue insider or just a user from making a mistake, ensuring that your intellectual property is not compromised.
- **ESTABLISHING** a normal behavior baseline, giving you early indications of a potential risk when a user begins to stray for their normal activity.
- **PROVIDING CONTEXT** into a user's behavior, aiding your investigation.
- **IDENTIFYING** your riskiest users. An over the shoulder view enables you to put context around risky behavior, determining whether the employee action was malicious or accidental, or if the system was hijacked.

For more information on how Forcepoint and SureView Insider Threat can help you comply with NISPOM Change 2, contact us at nispominfo@forcepoint.com.

CONTACT
www.forcepoint.com/contact