SOLUTIONS SHEET

DIGITAL GUARDIAN®

For Automated NISPOM 2 Compliance

CONTRACTORS ARE REQUIRED TO ESTABLISH AND MAINTAIN AN INSIDER THREAT PROGRAM

INDUSTRIAL SECURITY
LETTER

ISL 2016-02

"On May 18, 2016, the Department of Defense published Change 2 to DoD 5220.22-M, 'National Industrial Security Operating Manual (NISPOM).' NISPOM Change 2 requires contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats. Contractors must have a written program plan in place to begin implementing insider threat requirements of Change 2 no later than November 30, 2016."

ACHIEVE NISPOM 2 FULL COMPLIANCE FASTER AND WITH GREATER CONFIDENCE

As part of the NISPOM process, you'll need to put reporting mechanisms in place that can fulfill the mandate without disrupting or duplicating your existing systems and ways of working. Digital Guardian offers an Insider Threat Managed Security Program that can address the documentation requirements implied in 1-202a, 1-300, and 1-304, as well as provide the user activity monitoring required by 8-100d.

It's designed to work with the data flows your organization already produces, and its report capabilities can serve as a core platform for the mandate's required documentation processes.

Our Managed Security Program can help ensure you meet the November 30th, 2016 deadline.

NISPOM CHANGE 2 REQUIREMENT FOR CONTRACTORS	DIGITAL GUARDIAN MANAGED SECURITY PROGRAM CAPABILITY
Gather, integrate, and report relevant and credible insider threat information covered by any of the 13 personnel security adjudicative guidelines	✓
Deter cleared employees from becoming insider threats	✓
Detect insiders who pose a risk to classified information	✓
Mitigate the risk of an insider threat	✓
Implement user activity monitoring on classified information systems to detect activity indicative of insider threat behavior	✓
Screen capture, key-logging and file capture of user activity	✓

DIGITALGUARDIAN®

For more information, visit
www.digitalguardian.com

DESIGNED FOR FEDERAL OPERATING ENVIRONMENTS

INFRASTRUCTURE AGNOSTIC SECURITY

Digital Guardian is ideally designed to support classified information security within complex operating restrictions. It is an autonomous, host-based security system that works equally well in physical and virtual environments to monitor and control file, application, and system operations independent of user status.

RISK-BASED POLICY ENFORCEMENT

Digital Guardian's advanced security agents operate in kernel and user-modes simultaneously for precise situational and threat awareness. Agents autonomously confirm potential threats defined by policy – and determine the correct enforcement response – using on-board logic relating user identity, clearance level, file classification, and mission scope.

SUPPORTS USER, APPLICATION, AND FILE-LEVEL CONTROLS

Once users are authorized to access protected data, Digital Guardian allows them to perform a wide range of file and application operations based on file classification and user clearance, ranging from copy/move/save as to removable media, upload, email, print, burn to CD, copy and paste, etc. Digital Guardian Insider Threat solutions support "share-to-win" policies out-of-the-box by monitoring and controlling user-level access to data, while also protecting and deterring unauthorized uses once a file has been accessed.

Gartner®
Magic Quadrant Leader
Enterprise Data Loss Prevention

COMPLEMENTS EXISTING IA/CND TOOLS AND ADDRESSES LE/CI NEEDS

Digital Guardian's tamper-resistant agents record situationally-aware and causal event logs with admissibility and weight precedence as primary forensic evidence in criminal and civil cases, both domestically and internationally.

SMALL BUSINESS
CERTIFIED

COMPREHENSIVE INSIDER THREAT INSIGHT AND CONTROLS

- Integrated software platform for insider threat monitoring, detection, deterrence, and prevention
- Provides continuous, rules-based capture of system activity as sequenced, compressed, hashed, signed, and encrypted log events
- Proven to scale beyond 500,000 agents reporting continuously to a single backend server
- Multi-tier reporting supports tactical or centralized CND analysis, and restricted LE/CI access
- Low load on network (50-200KB per user/per day of log data); communicates from anywhere in the world on any port over HTTP(S)
- Tamper-resistant agent sources own forensic data with kernel, user mode, and application layer visibility
- Hardened agent with configurable stealth and tamper resistance
- Data usage and movement monitoring and control addresses "share-to-win" requirements
- Provides cross domain data transfer assurance and accountability through monitoring and controlling transmit and receive points
- User anomaly detection with statistical analytics and optimized OLTP data warehouse
- Integrated, on-board AES 256-bit encryption for transparent or password-based file transfers; includes automated key management and recovery
- FIPS 140-2 certified cryptography
- Infrastructure agnostic, operates in physical or virtual/VDI environments
- Archived log data can be replayed for forensic, investigative or evidentiary purposes

Email **nispom2@digitalguardian.com** to learn how we can help ensure you meet the November 30th deadline.

ABOUT DIGITAL GUARDIAN

Digital Guardian is the only data aware security platform designed to stop data theft. The Digital Guardian platform performs across traditional endpoints, mobile devices and cloud applications to make it easier to see and stop all threats to sensitive data.

Digital Guardian Public Sector
12020 Sunrise Valley Dr., Suite 350
Reston, VA 20191

SHARE