SmartSuite

Framework / Supply Chain Security / Other

NISPOM (DoD 5220.22-M)

NISPOM prescribes security requirements and procedures for protecting classified U.S. government information in contractor facilities.

What it is

The National Industrial Security Program Operating Manual (NISPOM) is a U.S. federal regulatory framework that helps organizations safeguard classified information in support of national security objectives. NISPOM establishes uniform standards for the protection, handling, and control of classified information by government contractors, vendors, and other covered entities.

Published by the U.S. Department of Defense (DoD), NISPOM is binding on all federal agencies and private organizations participating in the National Industrial Security Program (NISP). The framework addresses a wide range of requirements, including personnel security, physical security controls, cybersecurity measures, incident reporting, risk management, and compliance oversight for classified contracts.

At a glance

PUBLISHER U.S. Department of Defense (DoD)	TYPE Regulation	VERSION 2020
EFFECTIVE February 24, 2021	DOMAIN Supply Chain Security	FAMILY Other
REGION United States	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY Very High		

Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf?ver=2019-06-06-145530-170

Why it matters

- **Strengthen information protection** Ensure robust safeguards for classified data, reducing unauthorized disclosure risks within defense-related operations.
- **Improve regulatory compliance** Align security practices with federal requirements, simplifying compliance efforts and supporting longstanding government contracts.
- **Enhance security oversight** Establish clear roles and responsibilities that improve accountability and management of industrial security protocols.
- **Promote operational resilience** Support business continuity by requiring incident response planning and recovery capabilities for classified program disruptions.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NISPOM (DoD 5220.22-M)

Classified Security Control Library

Structure NISPOM security requirements covering personnel, facility, information system, and operational safeguards.

Clearance and Personnel Security Management

Track personnel clearances, roles, and eligibility for accessing classified information and secure systems.

Classified System and Facility Governance

Manage systems, networks, and facilities handling classified information within approved security boundaries.

Insider Threat and Incident Tracking

Track potential security violations, insider threat events, and incident reporting requirements.

Classified Program Contractor Monitoring

Monitor contractors, subcontractors, and partners participating in classified government programs.

Security Program Reporting and DCSA Audit Readiness

Provide dashboards summarizing compliance status, open findings, and readiness for Defense Counterintelligence and Security Agency (DCSA) reviews.

Common framework mappings

CIS Controls v8.1 | CMMC 2.0 | Cyber Essentials | ISO 27001:2022 | NERC CIP | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2 | TISAX ISA v6

Official resources

NISPOM Main Manual

Provides comprehensive guidelines for safeguarding classified information within U.S. defense industry.

dcsa.mil/mc/ctp/nispom

NISPOM Rule Change Summaries

Outlines updates and changes to the National Industrial Security Program Operating Manual.

dcsa.mil/mc/ctp/nispom/rule

NISPOM Training Aids

Defines training requirements and offers official tools for NISP compliance.

dcsa.mil/mc/ctp/nispom/training

Frequently asked questions

What is NISPOM used for?

NISPOM establishes the requirements, policies, and procedures for safeguarding classified information within the U.S. defense industrial base. It guides contractors, government agencies, and personnel on handling classified information, facility clearance, and personnel security clearances to protect national security interests.

Is NISPOM compliance mandatory for contractors?

Yes, compliance with NISPOM is mandatory for all government contractors and subcontractors who need access to classified information as part of federal contracts. Non-compliance can result in loss of facility clearance, contract termination, or legal penalties.

What is the scope of NISPOM applicability?

NISPOM applies to all U.S. contractors, cleared facilities, and individuals who require access to classified information under the National Industrial Security Program. The requirements cover physical, personnel, and information security controls for classified contracts.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What key artifacts and documentation does NISPOM require?

NISPOM requires organizations to maintain a range of documentation, including Facility Security Clearance (FCL) records, personnel clearance files, Standard Practice Procedures (SPPs), self-inspection reports, and records of security violation investigations. These artifacts support proper implementation and demonstrate compliance during audits.

How do organizations implement NISPOM requirements?

Organizations implement NISPOM by developing internal security programs, designating Facility Security Officers (FSOs), training personnel, and establishing procedures for classified information handling. Periodic self-inspections, corrective actions, and ongoing oversight by Defense Counterintelligence and Security Agency (DCSA) are also required.

How does NISPOM relate to other security frameworks?

NISPOM is specific to the protection of classified information in the U.S. defense industrial base but aligns with principles from other frameworks like DoD 5220.22-M and some international security protocols. However, NISPOM focuses on national security information, while others may address broader information or physical security concerns.

What are ongoing NISPOM compliance requirements?

NISPOM requires continuous adherence to security controls, routine training, regular self-inspections, timely incident reporting, and prompt remediation of deficiencies. Organizations must also stay up-to-date with NISPOM updates and promptly implement changes to maintain compliance.

How would SmartSuite support NISPOM?

SmartSuite can help organizations manage NISPOM by providing centralized risk tracking, automated control management, and systematic evidence collection for compliance filings. It enables audit readiness through workflow management and documentation, facilitates incident reporting, and supports comprehensive reporting for continuous monitoring and oversight.

License included / downloadable: Yes The NISPOM is published by the U.S. DoD (DCSA) and is publicly available for download from official DoD/DCSA publications. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-nispom-national-industrial-security-program-operating-manual