PIM Form Resources

Page Contents

Jump to...

M Form Resources

'e

PIM Forms

Exostar's Partner Information Manager (PIM) offers a variety of forms. Please select from the following to review form descriptions, resources, and additional information:

- Conflict Minerals
- Concise DFARS / DFARS 252 CS
- Cyber Supply Chain Risk Management Questionnaire (CSCRMQ)
- CyberSecurity Questionnaire (CSQ)
- NIST SP 800-171

Please see the PIM Form Scoring page for information on how each form is scored.

Center for Internet Security (CIS) Controls

- CIS Controls ver 5.1
- CIS Controls latest version
- CIS Controls FAQs

CMMC

- CMMC DoD
- CMMC Accreditation Body
- CMMC Docs
- Exostar CMMC website
- Exostar CMMC Linkedin
- CERT RMM v1.2

Conflict Minerals

The Conflict Minerals Reporting Template is a free, standardized reporting template developed by the Conflict-Free Sourcing Initiative, which facilitates the transfer of information through the supply chain, regarding mineral country of origin and utilized smelters and refiners. The questionnaire is used to determine if suppliers are using smelters recognized by and meeting the CFSI standards. Please see the Conflict Minerals resources:

- Conflict Free Sourcing Initiative
- Conflict Minerals SEC Regulations
- Conflict Minerals Form Completion

Update Conflict Mineral Form Resources

The resources listed in the form template are currently out-of-date, please use the resources listed above.

Concise DFARS / DFARS 252 CS

The Concise DFARS form gives buying organizations a high level snapshot of a supplier's NIST compliance and CDI flow down obligations. Buyers can now make a decision as to whether or not they need specific suppliers to submit a full NIST form, with answers to all 110 controls. Please see the Concise DFARS Form resources:

- DFARS 252 CS Blank Form
- DFARS 252 CS Form Completion

Cyber Supply Chain Risk Management Questionnaire (CSCRMQ)

The questions in this form are based on the operational requirements of the NIST SP 800-161 standard, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities.

Please see CSCRMQ resources:

- Computer Security Resource Center
- CSCRMQ Blank Form
- CSCRMQ Completion

CyberSecurity Questionairre

The Cybersecurity Questionnaire was developed to measure a Supplier's cybersecurity capability. The information a Supplier Partner provides helps them understand their organization's cybersecurity posture. The questionnaire also helps Buying Partners manage risks with sharing sensitive information. Please see CSQ resources:

- DIB SCC Cyber Assist
- CSQ Blank Form
- CSQ Form Completion

NIST SP 800-171

The Department of Defense (DoD) now requires all its contractors to protect Covered Defense Information (CDI). The department modified its Defense Federal Acquisition Regulation Supplement (DFARS) to address the safeguarding of CDI. The DFARS clause 252.204-7012 requires *covered companies* t o use the cyber safeguards described by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-171, which NIST created specifically for commercial companies who do not operate *federal information systems*, but who receive or create CDI to perform defense contracts. The information a Supplier Partner provides in the NIST SP 800-171 questionnaire is used by Buying Partners to determine a business's security posture with respect to the required NIST security controls. Please see NIST Form resources:

- NIST 800-171, rev 2
- NIST 800-171, rev 1
- NIST 800-171A
- NIST 800-171B draft
- NIST MEP Cybersecurity Self-Assessment Handbook
- DFARS 252.204-7012
- NIST SP 800-171 Controls References
- NIST SP 800-171 DoD Assessment Methodology
- NIST Blank Form
- NIST Form Completion

Additional Resources

- NIST Cryptographic Module Validation Program (CMVP)
- NIST Supply-chain Risk Management
- NIST Cyber Security Framework
- NIST 800-53 rev.5 draft

- NAICS Association (NAICS Codes)
- United Nations Standard Products and Services Code (UNSPSC)
- Sustainable Marketplace and Green Products

How useful was this content?

Your Rating: Results: 10 rates