DoW Instruction 3000.19

General Procedures for Vendor Threat Mitigation

Originating Component:	Office of the Under Secretary of War for Acquisition and Sustainment
Effective:	February 2, 2026
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Approved by:	Michael P. Duffey, Under Secretary of War for Acquisition and Sustainment

Purpose: In accordance with the authority in DoD Directive (DoDD) 5135.02 and the guidance in DoDD 3000.16, this issuance establishes policy, assigns responsibilities, and provides procedures for vendor threat mitigation (VTM).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 4
1.1. Applicability. 4
1.2. Policy. 4
1.3. Information Collections. 6
SECTION 2: RESPONSIBILITIES 7
2.1. Under Secretary of War for Acquisition and Sustainment (USW(A&S)). 7
2.2. Deputy Assistant Secretary of War for Logistics (DASW(LOG)). 7
2.3. Principal Director, DPCAP. 8
2.4. Under Secretary of War for Research and Engineering. 9
2.5. Under Secretary of War for Policy (USW(P)). 9
2.6. DASW(DC&MA). 9
2.7. Assistant Secretary of War for Special Operations and Low-Intensity Conflict. 9
2.8. USW(I&S). 9
2.9. Director, Defense Intelligence Agency. 11
2.10. IG DOD. 11
2.11. ATSW(PCLT). 11
2.12. DoW Component Heads. 11
2.13. DoW Component Heads, Not Including CJCS or CCDRs. 12
2.14. Secretaries of the Military Departments. 12
2.15. CJCS. 12
2.16. CCDRs. 13
SECTION 3: VTM STANDARDS AND PROCEDURES 14
3.1. Terminology Clarification. 14
3.2. VTM Program Management. 14
a. Scope and Applicability. 14
b. Policy and Guidance. 15
c. Deconfliction and Escalation of Issues. 15
d. Re-vetting. 15
e. Planning Considerations and Requirements. 15
f. Program Oversight. 15
g. Interagency Coordination. 16
h. Coordination to Support Executing VTM Functions. 16
3.3. VTM Functions. 16
a. Vetting. 16
b. Risk Assessment. 16
c. Risk Management. 16
d. Information Sharing. 17
3.4. Vetting. 17
3.5. Risk Assessment. 18
3.6. Risk Management. 19
3.7. Information Sharing and Data Storage. 21
a. Overview. 21
b. Information Sharing. 22

c. Data Storage. 22
3.8. Reporting 23
GLOSSARY 25
G.1. Acronyms. 25
G.2. Definitions. 26
REFERENCES 28

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSW, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), the Office of Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoW Field Activities, and all other organizational entities within the DoW (referred to collectively in this issuance as the "DoW Components").

b. This issuance does not apply to vendors that are covered entities under Part 117.2(a)(3) of the Code of Federal Regulations also known as the National Industrial Security Program Operating Manual.

1.2. POLICY.

a. VTM programs will be established and maintained in each CCMD, and may be established and maintained in other DoW Components, to:

(1) Vet, assess, and manage risk posed by vendors that are engaging in covered activities and:

(a) Disrupt and degrade foreign intelligence entities, violent extremist organizations, or criminal control, influence, or exploitation of commercial support to DoW operations.

(b) Deny, disrupt, or degrade opportunities of foreign intelligence entities, violent extremist organizations, transnational crime organizations, or other entities hostile to the U.S., allied, and partner interests for espionage, sabotage, coercion, and provision of materiel or other resources through commercial support to operations.

(c) Protect U.S., allied, and partner personnel, equipment, supplies, and installations from acts of foreign intelligence entities, violent extremist organizations, transnational crime organizations, or other hostile entities that result in espionage, sabotage, infiltration, or other threats resulting from exploitation of commercial support to operations.

(2) Enable cross-functional coordination between Combatant Commanders (CCDRs) and other DoW Component heads to make informed decisions that consider the risks associated with using commercial support, including collaboration between the contracting, finance, intelligence, law enforcement (LE), security, legal, and mission assurance communities.

b. Assessments of beneficial ownership and foreign ownership, control, or influence will be referred to the Defense Counterintelligence and Security Agency in accordance with DoD Instruction (DoDI) 5205.87, when applicable.

c. Assessments of mission critical acquisitions will be referred to the DoW Supply Chain Risk Management Threat Analysis Center to complete threat assessments in accordance with DoDIs 4140.01, 5000.86, 5200.44, 5240.18, and O-5240.24.

d. System security and cybersecurity technical risks will be managed in accordance with DoDI 5000.83 and critical program information protection will be managed in accordance with DoDI 5200.39.

e. Due diligence for Small Business Innovation Research program and Small Business Technology Transfer program proposals and awards will comply with the May 13, 2024 Deputy Secretary of Defense Memorandum.

f. Intelligence or intelligence-related activities in support of VTM will be conducted in accordance with DoDD 5240.01 and in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons. All defense intelligence and intelligence-related activities in support of VTM will be conducted in accordance with applicable laws, Executive orders, Presidential directives, Intelligence Community directives (ICDs), or applicable DoW policy governing the activity including, but not limited to:

(1) Intelligence oversight guidance established in DoDD 5148.13.

(2) ICDs 203, 206, 208, 209, and 501.

(3) DoD Manual (DoDM) 5240.01.

g. Classified information used to support VTM may not be disclosed to a vendor, or their representatives, in the absence of a protective or confidentiality order issued by a court of competent jurisdiction established in accordance with Article I or Article III of the Constitution of the United States of America that specifically addresses the conditions upon which such classified information may be disclosed, in accordance with DoDI 5200.48 and Sections 1- through 16 of Title 18a, United States Code (U.S.C.), also known as the "Classified Information Procedures Act," as amended, or another lawful purpose for disclosure.

h. Controlled unclassified information must be marked in accordance with existing guidance and will only be authorized for public release in accordance with DoDIs 5200.48, 5230.09, and 5230.29, or DoDM 5400.07.

i. In accordance with DoDI 5400.04, nothing in this issuance will prohibit the DoW from sending controlled unclassified information to Congress in accordance with DoDI 5200.48 or will prevent the DoW from meeting its statutory responsibilities under Section 501 of the Intelligence Oversight Act of 1980 to keep the congressional intelligence committees fully and currently informed of all intelligence activities that are carried out by the DoW or its intelligence agencies.

j. Acquisition decisions, including vendor eligibility and contract award, remain the sole responsibility of contracting officers in accordance with applicable statutes and regulations.

k. Nothing in this issuance will infringe on IG DoD or Defense Intelligence Component Inspectors General statutory authority in accordance with Chapter 4 of Title 5, U.S.C., also known and referred to in this issuance as the "Inspector General Act." In the event of any conflict between this issuance and IG DoD or Defense Intelligence Component Inspectors General statutory authority, the Inspector General Act takes precedence.

1.3. INFORMATION COLLECTIONS.

Collection of the information required to support VTM has been assigned Office of Management and Budget Control Numbers 9000-0159 and 0704-0589, in accordance with the procedures in Volume 2 of DoDM 8910.01. The expiration date of this information collection can be found on the Office of Management and Budget website at https://www.reginfo.gov/public/do/PRASearch.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF WAR FOR ACQUISITION AND SUSTAINMENT (USW(A&S)).

The USW(A&S) acts as the Principal Staff Assistant and principal civilian advisor to the Secretary of Defense for VTM in accordance with DoDD 3000.16 and develops and implements DoW policy, tools, and communications for the VTM Program in coordination with the Under Secretary of War for Intelligence and Security (USW(I&S)).

2.2. DEPUTY ASSISTANT SECRETARY OF WAR FOR LOGISTICS (DASW(LOG)).

Under the authority, direction, and control of the USW(A&S), through the Assistant Secretary of War for Sustainment, the DASW(Log):

a. Develops policy and governance to implement VTM in the DoW by:

(1) Overseeing implementation of VTM capabilities and activities in coordination with the DoW Component heads.

(2) Supporting the USW(I&S) on intelligence, security, and LE matters related to implementing VTM activities.

b. In conjunction with the USW(I&S), validates the requirements necessary to execute VTM processes and submits validated requirements to relevant DoW forums, such as: systems configuration control boards; the Planning, Programming and Budgeting Execution process; or other joint requirements validation processes, as needed.

c. In coordination with the DoW Component heads, establishes guidance for identifying and using VTM-related information and facilitates sharing VTM-related information within the DoW, and with other U.S. Government agencies.

d. In coordination with the USW(I&S), the Principal Director, Defense Pricing, Contracting, and Acquisition Policy (DPCAP), and the DoW Component heads, oversees management of the information necessary to execute VTM programs.

e. In coordination with the USW(I&S), the Principal Director, DPCAP, the Deputy Assistant Secretary of War for Defense Continuity and Mission Assurance (DASW(DC&MA)), and the CJCS, supports the development of VTM training and education requirements.

f. In conjunction with the Principal Director, DPCAP, and in coordination with the DoW Component heads, identifies and advocates for authorities to close capability gaps or advance VTM policy goals, if required.

g. Co-chairs the VTM Executive Council and subordinate working groups in accordance with the VTM Executive Council and Working Group Charter.

h. In coordination with the CJCS, facilitates the deconfliction and resolution of VTM-related capability development and risk management issues upon escalation by the CCDRs or other DoW Component heads.

i. Identifies and establishes criteria for skill sets required by military and civilian personnel to perform VTM functions.

2.3. PRINCIPAL DIRECTOR, DPCAP.

Under the authority, direction, and control of the USW(A&S), through the Assistant Secretary of War for Acquisition, the Principal Director, DPCAP:

a. Coordinates with applicable regulatory councils to update acquisition regulations, including the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement, to implement VTM requirements and issues contracting policy, guidance, and procedures to implement VTM requirements, as needed.

b. Identifies gaps in acquisition-related data necessary to execute VTM; advocates for and supports implementation of solutions to enable VTM, including the establishment of a system to house vendor data necessary for VTM programs.

c. In coordination with the DASW(Log) and with DoW Component heads, ensures that the development and use of contract clauses and procurement guidance support execution of VTM programs and that VTM program guidance considers limitations of acquisition regulations and authority.

d. In coordination with the DoW Component heads, supports the DASW(Log) in overseeing management and sharing of acquisition-related information necessary to execute VTM programs.

e. In coordination with the DASW(Log), and the DoW Component heads, develops training and education requirements for the acquisition workforce on VTM-related policies and advises on the application of these training and educational requirements to the acquisition workforce, including compliance with acquisition regulations and authority.

f. In conjunction with the DASW(Log):

(1) Develops and maintains processes and procedures for reporting on the use of acquisition authorities to support VTM programs, as needed.

(2) Advocates for authorities to close acquisition capability gaps or advance acquisition-related VTM policy goals, if needed.

2.4. UNDER SECRETARY OF WAR FOR RESEARCH AND ENGINEERING.

The Under Secretary of War for Research and Engineering develops policy and processes to govern DoW assistance awards under its authority and incorporates VTM requirements into related policy and processes, where applicable.

2.5. UNDER SECRETARY OF WAR FOR POLICY (USW(P)).

The USW(P) assesses the impact of potential VTM-related risk management actions on current U.S. national security policy and coordinates with the USW(A&S), the USW(I&S), the CJCS, and other DoW Component heads on courses of action for risk management.

2.6. DASW(DC&MA).

Under the authority, direction, and control of the USW(P), through the Assistant Secretary of War for Homeland Defense and Hemispheric Affairs, the DASW(DC&MA) oversees the incorporation of anti-terrorism and force protection-related activities into CCDR VTM programs in coordination with the CJCS.

2.7. ASSISTANT SECRETARY OF WAR FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT.

In accordance with the authority in DoDD 5111.10, the Assistant Secretary of War for Special Operations and Low-Intensity Conflict:

a. Integrates VTM doctrine, policy, and guidance into United States Special Operations Command and irregular warfare policy, programming, training, and operational support.

b. Integrates VTM into special operations and irregular warfare training and education.

c. Assesses the resources required to support United States Special Operations Command VTM program requirements and assesses any resource shortfalls.

d. Integrates VTM into special operations and low-intensity conflict exercises.

2.8. USW(I&S).

The USW(I&S):

a. In coordination with the USW(A&S), the CJCS, and the Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency (ATSW(PCLT)), establishes policy, guidance, and oversight on developing and implementing DoW-wide VTM policies, processes, procedures, and guidelines to support intelligence, LE, and security-related VTM activities.

b. In conjunction with the USW(A&S), validates the capability development requirements necessary to execute Defense Intelligence Enterprise (DIE) and Defense Security Enterprise (DSE) activities relating to intelligence support for the execution of VTM and submits validated requirements to relevant DoW forums such as systems configuration control boards; the Planning, Programming and Budgeting Execution process; or other joint requirements validation other processes, as needed.

c. In coordination with DIE and DSE stakeholders, oversees and coordinates the development and implementation of VTM intelligence, LE, and security functions in accordance with DoDD 5143.01 and the April 21, 2023 Deputy Secretary of Defense Memorandum by:

(1) Establishing policy, priorities, and guidance for DoW LE support to VTM activities in his or her capacity as the Principal Staff Assistant for DoW LE.

(2) Overseeing intelligence, counterintelligence (CI), security, and LE matters related to VTM.

(3) Overseeing and advocating for intelligence, CI, security, and LE-related Military Intelligence Program and non-Military Intelligence Program resources and manpower requirements for effective support to VTM activities, in accordance with DoDDs 3000.16 and 5205.12, and DoD 7000.14-R.

d. In coordination with the DASW(Log), the Principal Director, DPCAP, and the CCDRs, oversees management of the security information and intelligence necessary to execute VTM programs (e.g., threat assessments).

e. Coordinates with the DASW(Log) on intelligence, security, and LE matters related to implementing VTM activities.

f. Establishes guidance for VTM information sharing and implements and maintains VTM information sharing capability within the DIE and the DSE.

g. In coordination with the CJCS and DIE and DSE stakeholders, oversees the development of requirements for DoW training and education on intelligence and security support for VTM.

h. In coordination with the USW(A&S), the CJCS, and functional owners, develops DoW-wide training and education guidelines for DIE, DSE, and LE support to VTM.

i. In coordination with the DoW Component heads, establishes guidance for sharing VTM-related intelligence, LE, and security information with U.S. allies and partners.

j. Develops and implements DoW policy, tools, and communications on VTM intelligence, intelligence-related and security activities in coordination with the USW(A&S)).

2.9. DIRECTOR, DEFENSE INTELLIGENCE AGENCY.

Under the authority, direction, and control of the USW(I&S), and in addition to the responsibilities in Paragraphs 2.12. and 2.13., the Director, Defense Intelligence Agency:

a. Advocates for all-source intelligence and CI support to VTM programs.

b. Develops and maintains a VTM training program and integrates VTM into existing training programs for the DIE and for the DSE that support VTM in accordance with DoDIs 3305.02 and 5240.27.

2.10. IG DOD.

The IG DoD oversees and evaluates DoW Component compliance with this issuance as the IG DoD considers appropriate.

2.11. ATSW(PCLT).

The ATSW(PCLT) provides policy, advice, guidance, and oversight on matters of privacy, civil liberties, and intelligence oversight that involve VTM programs, systems, or data in accordance with DoDD 5148.13, DoDI 5400.11, and DoDM 5240.01.

2.12. DOW COMPONENT HEADS.

The DoW Component heads:

a. Coordinate with the USW(A&S), the USW(I&S), the USW(P), the DoW Component head(s) of contracting activities, and other stakeholders as needed to use appropriate authorities to assess threat and mitigate risks identified through their respective component's implementation of VTM policy.

b. Oversee implementation of their organization's responsibilities and procedures outlined in Section 3, as applicable.

c. Request information from the Director of the Defense Counterintelligence and Security Agency on vendors under foreign ownership control and influence in accordance with DoDI 5205.87 and integrate such information into their organization's threat and risk assessments, when applicable.

d. Adhere to CCMD VTM program requirements and ensure that supporting components and contracting officers consider VTM risk assessments when operating within a CCDR's area of responsibility (AOR).

e. In coordination with the other DoW Component heads, ensure that development and use of contract clauses and procurement guidance support execution of VTM programs and that VTM program guidance incorporates the requirements of acquisition regulations and authority.

f. Participate in the VTM Executive Council and subordinate working groups in accordance with the VTM Executive Council and Working Group Charter.

g. Adhere to the information-sharing requirements in Paragraph 3.7.

2.13. DOW COMPONENT HEADS, NOT INCLUDING CJCS OR CCDRS.

The DoW Component heads, not including the CJCS or the CCDRs, who implement VTM programs, should follow the procedures and standards established in Section 3 to the maximum extent practical, including required reporting in Paragraph 3.8.

2.14. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraphs 2.12. and 2.13., the Secretaries of the Military Departments:

a. Develop and integrate VTM doctrine, policy, and guidance into Military Department and Military Service policy, programming, training, and support to operations.

b. Integrates VTM in training and education for military and civilian personnel within the Military Departments.

c. Assess resources required to support CCMD VTM program requirements and assesses any shortfalls.

d. Identify or establish criteria for skill sets required by military and civilian personnel to perform VTM functions.

e. Integrate VTM into military exercises.

2.15. CJCS.

In addition to the responsibilities in Paragraph 2.12., the CJCS serves as the principal military advisor to the Secretary of War for VTM and:

a. Establishes and updates joint doctrine, instructions, manuals, and universal joint tasks for VTM.

b. Incorporates VTM into joint strategic planning guidance, where applicable.

c. In coordination with the USW(I&S), the DASW(Log), the DASW(DC&MA), and the Principal Director, DPCAP, supports development of VTM training and education requirements.

d. Through the Vice Director for Logistics J-4, co-chairs the VTM Executive Council and subordinate working groups in accordance with the VTM Executive Council and Working Group Charter.

e. Solicits, analyzes, and publishes joint lessons learned for VTM within the DoW.

f. In coordination with the DASW(Log), facilitates the deconfliction and resolution of VTM-related issues upon escalation.

2.16. CCDRS.

In addition to the responsibilities in Paragraph 2.12., the CCDRs:

a. Establish, oversee, and execute CCMD VTM programs, including assigning primary staffs responsible for carrying out the requirements in Section 3 and documenting these responsibilities in plans, orders, instructions, or other command guidance.

b. Identify and document requirements to resource and execute CCMD VTM programs.

c. In coordination with the USW(I&S), the DASW(Log), and the Principal Director, DPCAP, use acquisition, intelligence, LE, and security information to execute CCMD VTM programs.

d. Implement VTM training for CCMD primary and special staffs, as needed.

e. Report on VTM program execution annually to the USW(A&S) and the USW(I&S), including identifying shortfalls, readiness, outcomes of vetting processes, and lessons learned, and apply the appropriate remedies or changes to the VTM process to enhance threat and risk assessment, as required.

f. Integrate VTM into CCMD and joint exercises.

g. Participate in the VTM Executive Council and subordinate working groups in accordance with the VTM Executive Council and Working Group Charter.

h. Escalates VTM issues that have arisen within the CCMD's area of responsibility and that cannot be resolved by the CCDR and supporting components to the DASW(Log) and the CJCS for resolution through the VTM Working Group.

SECTION 3: VTM STANDARDS AND PROCEDURES

3.1. TERMINOLOGY CLARIFICATION.

As VTM programs are required in CCMDs and optional in the other DoW Components, direction in this section will refer to "CCDRs" and "CCMDs" and only refer to other DoW Components when the owner of the VTM program must interact with DoW Components outside their own. DoW Components other than CCMDs establishing VTM programs will follow the direction in this section to the maximum extent practical, substituting "DoW Component head" for "CCDR" and "DoW Component" for "CCMD."

3.2. VTM PROGRAM MANAGEMENT.

VTM program management is the process to identify and address potential risks to mission and forces associated with using commercial support to operations within the CCMD AOR. The CCDR will designate a VTM program manager to coordinate VTM information sharing across staff functions at various levels within the CCMD and supporting DoW Components. VTM program management is a continuous activity that underpins all other VTM functions within a CCMD. CCDRs should utilize VTM program management during all campaign, contingency, and crisis operations. VTM program management may vary by CCMD, but will at least include:

a. Scope and Applicability.

Under the direction of the CCDR, the VTM program manager will define the VTM program requirements, such as scope and applicability. VTM programs may vary in terms of scope and applicability based on mission set and requirements for contracted support. VTM program managers will prioritize vetting requirements based on commercial support requirements that introduce the greatest probability of risk to mission and forces; VTM programs are not required to vet all vendors that provide support in an AOR. VTM program managers consider multiple factors when determining whether a vendor should fall within the scope of a VTM program, such as:

(1) Estimated or actual dollar values of requirements or contracts.

(2) Force protection requirements.

(3) Mission assurance processes.

(4) Mission objectives and corresponding limitations.

(5) Adversaries and their capabilities and motivations.

(6) Critical capabilities to meet mission needs, and all possible sources of these capabilities.

(7) Available authorities to vet, identify, and address risks associated with contracted support within the AOR (e.g., acquisition authorities, force protection authorities).

(8) Availability of information on subcontractors.

b. Policy and Guidance.

The VTM program manager will develop and maintain VTM policy and guidance for the CCMD in coordination with other staffs and supporting components. The VTM program manager will work with the senior contracting officials throughout the DoW and the Principal Director, DPCAP, to develop and implement guidance that informs vendors of the CCDR program and its requirements.

c. Deconfliction and Escalation of Issues.

The VTM program manager will facilitate the deconfliction of vetting, risk assessment, and risk management activities, as necessary. Issues that cannot be resolved within the CCMD or between two or more CCMDs should be escalated to the DASW(Log) and the CJCS for assessment and resolution. The DASW(Log) and the CJCS will consult with the USW(I&S), the DASW(DC&MA), the Principal Director, DPCAP, and other organizations as necessary as part of the deconfliction process.

d. Re-vetting.

Periodic re-vetting of vendors will be determined by each CCMD based on its unique VTM program requirements. See Paragraphs 3.5.d. through 3.5.f. for additional information on re-vetting of vendors.

e. Planning Considerations and Requirements.

Campaign and contingency plans will include considerations for the VTM program that are applicable to the plans.

f. Program Oversight.

Oversight involves reviewing VTM program operations so that tasks are executed in accordance with applicable policy and guidance, and that risks are identified, vetted, and addressed through defined processes. Tasks associated with oversight of the VTM program include:

(1) Case Management.

The use of a case management approach for execution of VTM ensures that VTM processes are executed consistently for each vendor and in accordance with the procedures established in this issuance. The CCMDs that establish VTM programs may not always execute vetting functions systematically in accordance with a process that is sequential from case initiation to completion.

(2) Knowledge Management.

Within VTM programs, vendor information, such as risk assessments, along with risk management recommendations, must be stored and shared in accordance with VTM program guidelines, acquisition regulations, ICDs, and any other knowledge management standards that the VTM program manager deems relevant. Paragraph 3.7. includes additional information on information sharing and data storage.

(3) Reporting.

Oversight of VTM task execution should enable the VTM program to report on VTM activities as described in Paragraph 3.8.

g. Interagency Coordination.

VTM program managers will coordinate with stakeholders from other U.S. Government agencies, as well as allies and partners, through designated offices (e.g., the CCMD Interagency Partnering Directorate) to meet mission objectives. Coordination with stakeholders will be conducted in accordance with existing organization processes and applicable laws, regulations, and policies.

h. Coordination to Support Executing VTM Functions.

Where necessary, VTM program managers may need to provide support for executing VTM functions (e.g., vetting, risk assessment, and risk management) by facilitating decision-making between staff and with supporting components or conducting other collaborative activities with interagency, allies, and partners that improve VTM program performance.

3.3. VTM FUNCTIONS.

VTM programs will implement the following functions.

a. Vetting.

Leverage all-source intelligence analysis, including CI, LE, and security information, to identify threats posed by vendors to U.S. missions, forces, allies, and partners.

b. Risk Assessment.

Consider the threats identified through vetting vendors in the context of CCMD objectives to assess risk.

c. Risk Management.

Determine actions to address the risk associated with a particular vendor and coordinate the approval and execution of these actions with units that have a requirement for the vendor's support and contracting activities that acquire supplies and services from the vendor.

d. Information Sharing.

Share VTM-related information with other DoW Components, as well as with whole-of-government and U.S. allies and partners, when permissible under law, regulation, and policy and in appropriate cases.

3.4. VETTING.

Vetting involves assessing vendors and potential threats posed by those vendors that are subject to the VTM program. Vetting informs risk assessment and risk management. Vetting commences with all-source intelligence analysis of one or more vendors and concludes with a threat assessment that includes a threat rating. Vetting procedures will be conducted in accordance with applicable DIE and DSE policies.

a. Intelligence analysts will use all available sources of information to vet a vendor and:

(1) Analyze a vendor's connection to foreign intelligence entities, transnational organized crime or criminal activities, or other threat-related activities by conducting all-source intelligence analysis, including CI, counter threat finance analysis, and other security information.

(2) Identify the threat level a vendor poses to the United States and/or U.S. allies and partners as it pertains to the CCMD mission and equities.

(3) When LE-related concerns are identified, coordinate with the appropriate LE office to obtain additional input.

b. The threat presented by a vendor will be assessed as critical, high, medium, low, or unknown.

c. Threat assessments will:

(1) Consider threats posed by vendors, including prime contractors and subcontractors.

(2) Assign threat ratings based on guidance from the USW(I&S).

(3) Meet CCMD VTM program requirements, as well as requirements in applicable DIE and Intelligence Community policy including, but not limited to, DoDD 5148.13, DoDI O-5240.10, DoDM 5240.01, and ICDs 203, 206, 208, 209, and 501.

(4) Be shared with DoW stakeholders and other U.S. Government agencies and U.S. allies and partners at the appropriate classification level and with dissemination controls pursuant to applicable Intelligence Community policy.

d. CCDRs will define and assign roles and responsibilities for vetting through CCMD policy, orders, instructions, or other command guidance. CCDRs will resolve any conflicting staff priorities with respect to vetting responsibilities or outcomes, if required.

3.5. RISK ASSESSMENT.

a. VTM risk assessment will be conducted using the Joint Risk Analysis Methodology outlined in CJCS Manual 3105.01B and involves reviewing the threat assessment described in Paragraph 3.4. and information on the operational environment needed to assess the risks posed by vetted vendors. The VTM risk assessment process will be used to determine if a risk management action is necessary for award of a contract, grant, or cooperative agreement to a particular vendor.

(1) CCDRs commence the VTM risk assessment process by reviewing the applicable threat assessment, followed by reviewing information on the operational environment (e.g., strategic objectives, military capabilities, physical environment, and infrastructure), potential vendor performance requirements, the CCDR's risk tolerance, and other information that may be needed.

(2) The VTM risk assessment process concludes with assigning a VTM risk category to the vendor.

b. CCDRs may coordinate with or request assistance from an individual, office, working group, or other organizational construct with actions associated with evaluating risks and risk category determinations to support execution of VTM responsibilities.

c. VTM risk categories that CCDRs may assign to a vendor include:

(1) Insufficient Information.

The vendor was vetted, but there is insufficient information available for the vendor to be assigned a risk category. The vendor will be re-vetted as appropriate based on mission requirements.

(2) Acceptable.

The vendor was vetted, and sufficient information is available to determine that the risk posed by the vendor poses is acceptable to the mission and/or forces.

(3) Unacceptable Without Mitigation.

The vendor was vetted, and sufficient information is available to determine that the vendor poses an unacceptable risk to the mission and/or forces without actions to manage or mitigate the risk. Use of this vendor will require the CCMD to implement mitigation efforts to address potential risk to the mission and/or forces.

(4) Identified Pursuant to Section 841 Authority.

The vendor was vetted and has been identified by a CCDR pursuant to note preceding Section 4871, Subchapter III of Chapter 385, Title 10, U.S.C., to be a threat or pose a risk to the United States or its partners and allied missions and forces. The CCDR will notify the USW(A&S), the USW(I&S), and the USW(P) pursuant to note preceding Section 4871,

Subchapter III of Chapter 385, Title 10, U.S.C. (Section 841 Authority), of the identification of the vendor and the rationale for such identification.

d. Vendors assigned a risk category of "Insufficient Information" or "Acceptable" that seek to do business with the DoW will be re-vetted periodically. Such re-vetting is necessary so that the threat assessment remains current and is based upon the latest intelligence, security, and LE information, mission objectives, and potential contract performance requirements.

e. Any vendor assigned a risk category of "Unacceptable Without Mitigation" or "Identified Pursuant to Section 841 Authority" will be re-vetted annually by the CCDR that assigned the risk category to determine whether the threat(s) and risk assessment are still appropriate, or a new risk category should be assigned to the vendor based on current CCMD mission requirements and/or new vendor information. Following an initial re-vetting, if a vendor does not continue to seek to do business with the DoW, re-vetting may be deprioritized unless the vendor seeks to do business with the DoW in the future.

f. Triggers and processes for re-vetting will be specified in CCMD policy and orders.

3.6. RISK MANAGEMENT.

VTM risk management addresses threats posed by vendors considering the risk category assigned to the vendor by determining appropriate actions to accept, avoid, transfer, or mitigate risks and coordinating and executing those actions with relevant stakeholders within the DoW, other U.S. Government agencies, and/or U.S. allies and partners.

a. Risk management requires a completed threat assessment, assignment of a VTM risk category through the VTM risk assessment process, and other relevant information on the operational environment that informs assignment of the risk category. Risk management is a continuous activity while the DoW receives support from a vendor. Risk management actions taken to support VTM will be documented in accordance with CCMD VTM policy and the application of the requirements of any relevant authorities that are leveraged to address and to mitigate the risk.

b. CCDRs may choose to accept, avoid, transfer, or mitigate risks identified during the VTM risk assessment process.

c. Factors that influence risk management and recommendations made, and actions taken, to address and mitigate the risk include:

(1) Time (e.g., the urgency of meeting the requirement specified in a contract).

(2) Status of the contract (e.g., pre-award or post-award).

(3) Availability of other sources to meet the requirement.

(4) Potential for unintended consequences on other aspects of U.S. Government operations, including contracting actions supporting those operations.

(5) The availability of resources needed to meet the U.S. Government's requirements.

(6) The complexity of potential actions that are necessary to address the risk (e.g., security considerations, resources required, number of stakeholders involved, authorities required).

(7) Diplomatic or economic sensitivity.

(8) Potential for reputational harm to the vendor.

(9) Significant risk to the DoW or other CCMDs outside the identifying CCDR's AOR.

d. Risk management actions may require coordination with one or more of the following communities:

(1) Acquisition;

(2) Force protection;

(3) LE;

(4) CI;

(5) Security;

(6) Cyber; or

(7) Interagency.

e. Risk management actions will be documented, implemented, monitored, and reported in accordance with CCMD VTM policy and the requirements of the authority that supports the risk management action. CCDRs may use CCMD VTM policy to establish command-specific procedures to take a risk management action under an authority, when permissible, but will not replace or supersede existing procedures for the use of the authority.

f. CCDRs will coordinate risk management actions with senior contracting officials in accordance with CCMD VTM policy when such actions impact contracting authority and/or affect contracting support equities (e.g., pre-award, award, or post-award management of contract actions) and with security officials when such actions impact LE or force protection concerns.

g. The VTM program manager will assist in the coordination of risk management actions relating to specific vendors across the CCMD's concerned primary and special staffs or between components and component contracting activities. VTM program manager responsibilities include managing tasks associated with the VTM process to obtain input from CCMDs, DoW Component contracting activities, and other relevant stakeholders impacted or potentially impacted by actions taken as a result of the VTM risk assessment. VTM program manager responsibilities also include facilitating working groups to identify risk management actions and

developing recommendations or other courses of action as needed to mitigate risk to stakeholder missions and activities.

h. In situations in which risk is localized to a specific installation or geographical area, if the CCMD VTM policy allows it, the unit located at the installation or within the geographical area that is impacted by the risk assessment in terms of awarding contracts, grants, or cooperative agreements to a particular vendor may identify and implement risk management actions that only apply to that installation or geographical area.

i. It is possible the DoW may have multiple contracts (awarded under multiple contracting authorities) with a single vendor that provides support within an AOR, multiple AORs, or across multiple CCMD AORs. As a result, that single vendor may be assessed by multiple CCMD VTM programs and assigned multiple risk categories due to differences in CCMD mission and equites. A CCDR that is considering a risk management action for a vendor in such cases will:

(1) Share information with the DASW(Log), the Principal Director, DPCAP, the DASW(DC&MA), the CJCS, other CCDRs, DoW Component program officers, subordinate Component heads, and senior contracting officials at the DoW Components as necessary to determine if risk management actions under consideration will have an impact outside of their AOR.

(2) Coordinate risk management actions with all appropriate stakeholders, including the DASW(Log), the CJCS, other CCDRs, and DoW Component program officers.

3.7. INFORMATION SHARING AND DATA STORAGE.

a. Overview.

(1) Sharing VTM threat and risk assessments across the DoW ensures pertinent information is available for CCMD and other DoW Component risk assessments and risk management activities and maximizes use of resources in support of VTM.

(2) Standardizing data storage requirements for VTM information enhances information sharing across the CCMDs and the DoW Components. Information sharing is a continuous function included in VTM program management that supports all other VTM functions.

(3) As part of their VTM programs, CCDRs will share information and store data at the appropriate classification levels in accordance with applicable U.S. laws, regulations, and policy. Sensitive information, including information discovered on U.S. persons, as well as publicly and commercially available information on vendors, will be managed with appropriate mitigation and safeguards in accordance with DoDD 3115.18, DoDIs 5400.11 and 8320.02, DoDM 5240.01, Intelligence Community Policy Memorandum 504(01), or other applicable DoW policy such as DoDD 5200.27.

(4) Dissemination of VTM-related information outside of the DoW should be limited to persons having a valid need to know for acquisition, intelligence, CI, LE, finance, legal, mission

assurance, or related purposes. Such assessments may include sensitive information and should be handled in accordance with guidance for such material.

(5) The information sharing and data storage procedures established in this issuance are a minimum standard to encourage further coordination and collaboration between the CCMDs and the DoW Components as needed.

b. Information Sharing.

As part of their VTM programs, CCDRs are required to make the following information available to other DoW Component heads, in accordance with the requirements in Paragraph 3.8.:

(1) Vendors vetted (e.g., unique entity identifier or other company identifier and legal name).

(2) Threat rating and date(s) the vetting was completed.

(3) VTM risk categories assigned and summary of rationale.

(4) Company point of contact information and applicable key personnel.

c. Data Storage.

VTM programs will use common, searchable platforms at the appropriate classification level to make vendor-provided data, as well as vendor threat and risk information, available to contracting and non-contracting DoW personnel. Storage of data is subject to the requirements of DoDM 5240.01, when applicable. The information made available should include:

(1) Vendor Data.

CCMDs will obtain and make at least the following vendor data available to facilitate VTM functions:

(a) Company legal name.

(b) Company identifiers, such as government issued identifiers (e.g., unique entity identifier, Commercial and Government Entity or NATO Commercial and Government codes, or other government beneficial ownership identifiers) or foreign company identifiers, as available.

(c) Company point of contact information and applicable key personnel.

(d) Banking information.

(2) Threat Assessment.

Threat assessments will contain, at a minimum:

(a) General threat details.

(b) Threat rating.

(c) Confidence level.

(d) The date of completion for the most recent threat assessment.

(e) The date on which the request to vet a vendor was sent to the intelligence support component.

(3) Risk Assessments.

Risk assessments will contain, at a minimum:

(a) Original vetting organization.

(b) Risk category.

(c) The date the risk category was identified.

(4) Risk Management Information.

CCMDs will document risk management information, including risk management actions taken, and make such risk management information available to other DoW Component heads. Risk management information should be made available to other U.S. Government agencies and U.S. allies or partner stakeholders on an as-needed or as-permitted basis following CCMD processes and applicable laws, regulations, and policies.

3.8. REPORTING.

Reporting on execution of VTM programs will facilitate DoW-wide analysis to enhance understanding of global threats and risks faced by the DoW when it enters into contracts, grants, or cooperative agreements for commercial support. The USW(A&S) and the USW(I&S) will use the annual CCMD report outlined in this paragraph to develop and implement improvements to DoW policy, tools, and communications with DoW Components, other U.S. Government agencies, and U.S. allies and partners. CCDRs will report to the USW(A&S) and the USW(I&S) at least annually, or as requested, on VTM program execution. The annual CCMD report will be produced at the lowest appropriate classification level in accordance with the VTM Security Classification Guide and include at least:

a. The total number of vendors vetted per year, the risk categories assigned to each vendor, and what, if any, risk management actions were taken.

b. The corresponding risk assessment that includes the threat assessments for vendors identified as "Unacceptable Without Mitigation." Threat assessments will:

(1) Be reported to the USW(A&S) and the USW(I&S) at the lowest appropriate classification level.

(2) Include qualitative and quantitative analysis, such as description and frequency of the vendors' activities that cause the threats.

c. The number of vendors identified as "Unacceptable Without Mitigation" per year for which there were insufficient authorities available to effectively manage risk.

d. The number of vendors identified as "Unacceptable Without Mitigation" per year for which interagency or allies and partner authorities were used to manage the risk associated with that vendor (e.g., sanctions posed by the U.S. Department of the Treasury).

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AOR	area of responsibility
ATSW(PCLT)	Assistant to the Secretary of War for Privacy, Civil Liberties, and Transparency
CCDR	Combatant Commander
CCMD	Combatant Command
CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
DASW(DC&MA)	Deputy Assistant Secretary of War for Defense Continuity and Mission Assurance
DASW(Log)	Deputy Assistant Secretary of War for Logistics
DIE	Defense Intelligence Enterprise
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DoW	Department of War
DPCAP	Defense Pricing, Contracting, and Acquisition Policy
DSE	Defense Security Enterprise
ICD	Intelligence Community directive
IG DoD	Inspector General of the Department of Defense
LE	law enforcement
OSW	Office of the Secretary of War
U.S.C.	United States Code
USW(A&S)	Under Secretary of War for Acquisition and Sustainment
USW(I&S)	Under Secretary of War for Intelligence and Security
USW(P)	Under Secretary of War for Policy
VTM	vendor threat mitigation

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
AOR	The geographical or functional area associated with a CCMD within which the CCDR has authority to plan and conduct operations.
case	The process of identifying a vendor for vetting, vetting a vendor, generating a risk assessment, and determining risk management actions.
commercial support to operations	The risk-informed integration of commercial capabilities to meet mission requirements across the competition continuum.
covered activities	Defined in note preceding Subchapter III of Chapter 385, Title 10, U.S.C.
counter threat finance	Activities conducted to deny, disrupt, destroy, or defeat the generation, storage, movement, and use of assets to fund activities that support an adversary's ability to negatively affect U.S. interests.
Defense Intelligence Components	Defined in DoDM 5240.01.
DIE	Defined in DoDD 5143.01.
DSE	Defined in DoDD 5200.43.
intelligence	Defined in Executive Order 12333.
intelligence-related activities	Defined in DoDD 5240.01.
mitigation	Defined in DoDD 3000.16.
operational environment	A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.
prime contractor	Defined in DoDD 3000.16.
risk	Defined in CJCS Manual 3105.01B.

TERM	DEFINITION
subcontractor	Defined in DoDD 3000.16.
threat	Defined in DoDD 3000.16.
threat assessment	A determination of an entity's or individual's connection to activities harmful to national security.
vendor	Defined in DoDD 3000.16.
vet	Defined in DoDD 3000.16.
VTM	Defined in DoDD 3000.16.
VTM activities	Defined in DoDD 3000.16.
VTM functions	Groupings of similar VTM activities that occur in support of the VTM process.
VTM information	Any information required to execute a VTM function, including vendor information, threat assessments, risk categories, information required to determine a vendor's risk category, case management information, and documentation of risk management activities.
whole-of-government	Defined in DoDD 3000.16.

REFERENCES

The Constitution of the United States of America, September 17, 1787, as amended

Chairman of the Joint Chiefs of Staff Manual 3105.01B, "Joint Risk Analysis Methodology," December 22, 2023

Code of Federal Regulations, Title 32, Part 117.2(a)(3), "National Industrial Security Program Operating Manual (NISPOM)," December 21, 2020

Defense Federal Acquisition Regulation Supplement, current edition

Deputy Secretary of Defense Memorandum, "Designation of Principal Staff Assistant for Law Enforcement," April 21, 2023

Deputy Secretary of Defense Memorandum, "Defense Small Business Innovation Research and Small Business Technology Transfer Due Diligence Program," May 13, 2024

DoD 7000.14-R, "Department of Defense Financial Management Regulation (DoD FMR)"[1]

DoD Directive 3000.16, "Vendor Threat Mitigation," July 6, 2022

DoD Directive 3115.18, "DoD Access to and Use of Publicly Available Information (PAI)", June 11, 2019, as amended

DoD Directive 5111.10, "Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict," May 5, 2021, as amended

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))," July 15, 2020

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5148.13, "Intelligence Oversight," April 26, 2017

DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense", January 7, 1980

DoD Directive 5200.43, "Management of the Defense Security Enterprise," October 1, 2012, as amended

DoD Directive 5205.12, "Military Intelligence Program," November 27, 2024

DoD Directive 5240.01, "DoD Intelligence and Intelligence-Related Activities and Defense Intelligence Component Assistance to Law Enforcement Agencies and Other Civil Authorities," September 27, 2024

DoD Instruction 3305.02, "General Intelligence Training and Certification," August 12, 2015, as amended

DoD Instruction 4140.01, "DoD Supply Chain Materiel Management Policy," March 6, 2019

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended

DoD Instruction 5000.86, "Acquisition Intelligence," September 11, 2020

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015, as amended

[1] Available at https://comptroller.defense.gov/fmr/.

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," February 16, 2024

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5205.87, "Mitigating Risks Related to Foreign Ownership, Control, or Influence for Covered DoD Contractors and Subcontractors," May 13, 2024

DoD Instruction 5220.31, "National Industrial Security Program," May 9, 2023

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction O-5240.10, "Counterintelligence (CI) in the DoD Components," April 27, 2020

DoD Instruction 5240.18, "Counterintelligence (CI) Analysis and Production" November 17, 2009, as amended

DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended

DoD Instruction 5240.27, "Joint Counterintelligence Training Activity (JCITA)," November 13, 2013, as amended

DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017

DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections," June 30, 2014, as amended

Executive Order 12333, "United States Intelligence Activities," December 4, 1981

Federal Acquisition Regulation, current edition

Intelligence Community Directive 203, "Analytic Standards," January 2, 2015

Intelligence Community Directive 206, "Sourcing Requirements for Disseminated Analytic Products," January 22, 2015

Intelligence Community Directive 208, "Maximizing the Utility of Analytic Products," January 9, 2017

Intelligence Community Directive 209, "Tearline Production and Dissemination," September 12, 2012

Intelligence Community Directive 501, "Discovery and Dissemination or Retrieval of Information within the Intelligence Community," January 21, 2009

Intelligence Community Policy Memorandum 504(01), "Intelligence Community Policy Framework for Commercially Available Information," February 6, 2025

Joint Capabilities Integration and Development System Manual, "Manual for the Operation of the Joint Capabilities Integration and Development System," August 31, 2018

Intelligence Oversight Act of 1980[2]

United States Code, Title 5, Chapter 4

United States Code, Title 10, Chapter 385, Subchapter III

United States Code, Title 18a, Appendix III

Vendor Threat Mitigation Executive Council and Working Group Charter, current edition[3]

Vendor Threat Mitigation Security Classification Guide[4]

[2] https://www.congress.gov/bill/96th-congress/senate-bill/2284

[3] Available to authorized users at https://intelshare.intelink.gov/sites/atlcoi/vtm/SitePages/VTM_Working_Group.aspx.

[4]https://www.dtic.mil/document;accessionNumber=AD1325970;type=DTICTR;searchText=vendor%20threat%20mitigation%20security%20classification%20guide.