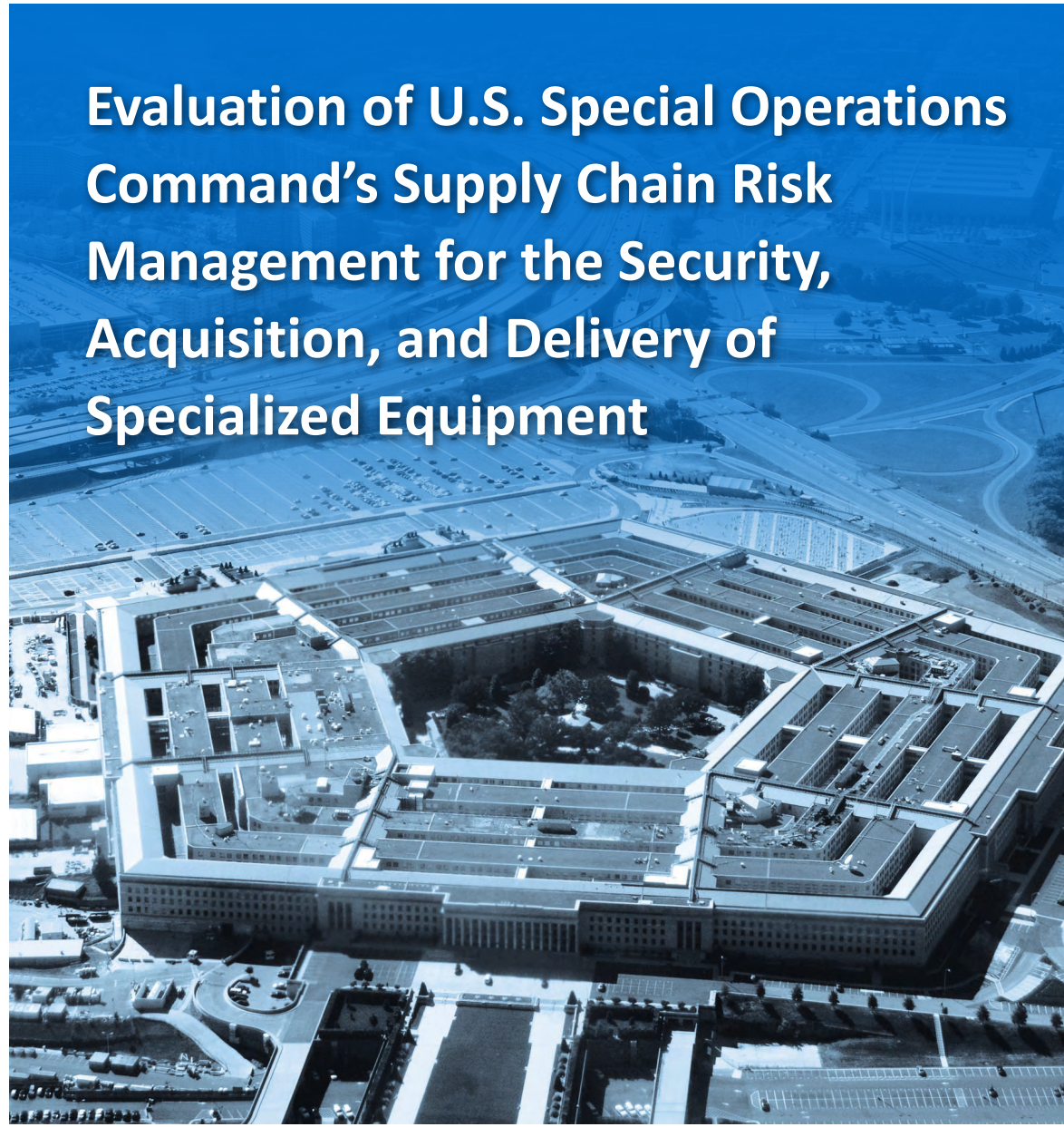




INSPECTOR GENERAL

U.S. Department of Defense

SEPTEMBER 14, 2021



Evaluation of U.S. Special Operations Command's Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE





**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500**

September 14, 2021

**MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH
AND ENGINEERING
ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS
AND LOW INTENSITY CONFLICT
COMMANDER, UNITED STATES SPECIAL OPERATIONS COMMAND**

SUBJECT: Evaluation of U.S. Special Operations Command's Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment (Report No. DODIG-2021-125)

This final report provides the results of the DoD Office of Inspector General's evaluation. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

The comments and associated actions taken by the Commander of U.S. Special Operations Command, Special Operations Forces Acquisition, Technology, and Logistics Center, addressed Recommendations 1.a and 1.b, and we consider those recommendations closed. The Commander agreed with Recommendations 2.a, 2.b, and 2.c and provided specific actions to address the recommendations; therefore, we consider those recommendations resolved but open.

As described in the Recommendations, Management Comments, and Our Response section of this report, we will close the recommendations when U.S. Special Operations Command provides us documentation showing that all agreed-upon actions to implement the recommendations are completed. Therefore, please provide us your response concerning specific actions in process or completed on the recommendations. Send your response to [REDACTED] if classified

SECRET. If you have any questions, please contact [REDACTED]

We appreciate the cooperation and assistance received during the evaluation.

Bryan Clark

Bryan T. Clark
Acting Assistant Inspector General for
Programs, Combatant Commands, and Overseas
Contingency Operations Evaluations



Objective

We determined the extent to which the U.S. Special Operations Command (USSOCOM) developed and implemented supply chain risk management procedures in accordance with DoD policy to identify, assess, and mitigate risk during the acquisition and development of USSOCOM specialized equipment. Specialized equipment is equipment, material, supplies, and services required for special operations missions for which there is no Military Service common requirement.¹

Executive Summary

In 2011, the DoD established policies that require DoD organizations authorized to procure materiel, services, and equipment to assess and mitigate threats, vulnerabilities, and disruptions to the DoD supply chain primarily through Program Protection Plans (PPPs). The USSOCOM Commander is authorized to develop and acquire specialized equipment and is required by policy to ensure supply chain security, such as anti-tampering and cyber, industrial, and information security. We found that USSOCOM supply chain risk management procedures did not comply with DoD policies until November 2020. Specifically, USSOCOM policy did not require USSOCOM program managers to complete PPPs for acquisitions programs, nor did USSOCOM policy require USSOCOM program managers to ensure that contractor-developed, program protection implementation plans (PPIPs) that address weaknesses identified PPPs were in place. While USSOCOM addressed these policy deficiencies in November 2020, USSOCOM personnel did not develop plans to prioritize and implement these policy requirements for active contracts. USSOCOM agreed with our two recommendations. One recommendation is closed, and the other recommendation is resolved but will remain open.

Background

According to Joint Publication 4-0, “the U.S. military supply chain (to include the defense industrial base) represents a major competitive advantage that underpins deterrence and allows the U.S. to project power.”² The defense industrial base consists of over 300,000 domestic and foreign companies who provide the DoD with the tools and capabilities needed to protect and secure the United States.³ Additionally, JP 4-0 states that the DoD’s supply chain reliability affects the readiness and capabilities of U.S. military forces and is critical to the overall

¹ Department of Defense, “DoD Dictionary of Military and Associated Terms,” January 2021. For this evaluation, we used the word *specialized* when referring to *Special Operations-peculiar* equipment.

² Joint Publication 4-0, “Joint Logistics,” May 2019.

³ DoD OIG, “Top Management Challenges,” October 2020.

success of globally integrated joint operations. The DoD supply chain is a global network that provides materiel, services, and equipment to the Services. The steps of the acquisition process include:

- identifying a need,
- manufacturing,
- purchasing,
- delivery,
- distribution,
- maintenance,
- repair,
- sustainment, and
- disposition.

Supply Chain Risk Management (SCRM) is the process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the DoD supply chain from beginning to end to ensure mission effectiveness. According to DoD Instruction 4140.01, successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the uninterrupted flow of product, materiel, information, and finances across the lifecycle of a weapon or support system.⁴

Developing and Implementing Supply Chain Risk Management Procedures

The DoD has provided guidance on developing and implementing SCRM procedures. Additionally, USSOCOM has developed detailed SCRM guidance based on DoD policy.

DoD Instruction 5000.02T Provides Policy for DoD Acquisitions

DoD Instruction (DoDI) 5000.02T establishes policy and procedures for managing acquisition programs under the relevant sections of title 10 United States Code and mandates the use of PPPs to address supply chain risk management.⁵ A PPP is the document developed by DoD program managers to help ensure protection measures for technology, components, and information are integrated and synchronized across programs. This protection, at a minimum, includes

⁴ DoD Instruction 4140.01, "DoD Supply Chain Material Management Policy," March 6, 2019.

⁵ DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 2015, is currently undergoing a revision process as specific policies are cancelled or transitioned to new DoD instructions. During the period of our evaluation, DoD Instruction 5000.02T, Change 10, December 31, 2020, was in effect. Program protection requirements transitioned from DoD Instruction 5000.02T to DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020 with Change 1, May 21, 2021. However, the portions of earlier versions of DoD Instruction 5000.02T relevant to our evaluation continue in the new DoD instruction.

anti-tampering, exportability features, cybersecurity, industrial security, information security, operations security, personnel security, and physical security, or equivalent countermeasures. Additionally, DoDI 5000.02T states that program managers will employ system security engineering practices and prepare a PPP to guide their efforts, and the actions of others, to manage the risks to Critical Program Information as well as mission-critical functions and components associated with the program.

DoD Instruction 5200.39 Provides Policy for Protecting Critical Program Information

DoDI 5200.39 establishes policy and assigns responsibilities for the identification and protection of Critical Program Information.⁶ Critical Program Information is the U.S. capability elements that contribute to the warfighters' technical advantage, which, if compromised, undermines U.S. military superiority. Additionally, DoDI 5200.39 states that DoD personnel will integrate and document critical information protection measures within PPPs in accordance with DoDI 5000.02T.

A Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum Provided Guidance for Program Protection Plans

On July 18, 2011, the Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics (PDUSD[AT&L]) issued a memorandum that provides formatting and content guidance for PPPs as required by DoDI 5000.02T and DoDI 5200.39.⁷ The guidance included managing risks to mission-critical system functionality from foreign collection, system design vulnerability, or supply chain exploitation. The memorandum also allows program managers to tailor PPP content to meet individual program needs and includes direction to align the prime contractor's PPIPs with the PPP.⁸ Finally, the memorandum requires every acquisition program to submit a PPP for management's review and approval at the first acquisition milestone and to update the PPP at each subsequent milestone.

⁶ DoD instruction 5200.39, "Critical Program Information Identification and Protection within Research, Development, Test and Evaluation," May 2015.

⁷ PDUSD (AT&L) Memorandum, "Document Streamlining-Program Protection Plan," July 2011.

⁸ A PPIP is the contractor-developed plan that serves as the principle communications means for validation and approval by the DoD or component program manager of the specific methods used by the contractor to identify the means chosen to implement the PPP at contractor, sub-contractor, and contractor-controlled locations and provide protection inputs to the system acquisition process.

U.S. Special Operations Command Directive 70-1 Provides Policy for Specialized Equipment

USSOCOM Directive 70-1 establishes policy for acquisition management of specialized equipment, material, supplies, and services in support of the USSOCOM mission and provides guidance for the use of PPPs for these acquisitions.⁹ Additionally, this directive defines the roles and responsibilities of USSOCOM personnel throughout the full life cycle of specialized equipment from requirements identification, to resourcing, to acquisition, and on through sustainment.

Roles and Responsibilities

USSOCOM is responsible for implementing DoD acquisition rules and regulations in its acquisition contracts. The USSOCOM Commander has delegated development and acquisition authority of specialized equipment to the office of Special Operations Forces Acquisition, Technology, and Logistics (SOF AT&L).

U.S. Special Operations Command

USSOCOM's mission is to develop and employ fully capable Special Operations Forces to conduct global special operations and activities as part of the Joint Force to support persistent, networked, and distributed combatant command operations and campaigns against state and non-state actors to protect and advance U.S. policies and objectives. The USSOCOM Commander has unique acquisition authorities and responsibilities. Section 167, title 10, United States Code, vests the USSOCOM Commander with the responsibility and authority for the development and acquisition of specialized equipment, the authority to exercise the functions of the head of agency, and the authority to execute funds. According to USSOCOM personnel, the USSOCOM Commander delegated those authorities to the USSOCOM Acquisition Executive, who leads SOF AT&L. Congress also provided USSOCOM with specific appropriation funding, Major Force Program-11, to support the development, acquisition, and sustainment activities for specialized equipment.

Special Operations Forces Acquisition, Technology, and Logistics

According to SOF AT&L officials, their mission is to provide rapid and focused acquisition, technology, and acquisition logistics support to USSOCOM's Service Components and Theater Special Operations Commands. To accomplish this mission, the SOF AT&L is comprised of the following nine Program Executive Offices (PEO):

- Command, Control, Communications, and Computers;
- Fixed Wing; Maritime;

⁹ United States Special Operations Command Acquisition, Technology, and Logistics Acquisition Management System Policy 70-1, November 18, 2020.

- Rotary Wing;
- Special Operations Forces Support Activity;
- Special Operations Forces Warrior;
- Special Reconnaissance, Surveillance, and Exploitation;
- Special Operations Forces Digital Applications; and
- Services.

Scope and Methodology

We conducted this evaluation from January 25, 2021, through June 30, 2021, in accordance with the “Quality Standards for Inspection and Evaluation,” published in December 2020 by the Council of Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that we meet objectives and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

We identified and reviewed the criteria that govern USSOCOM’s SCRM process. Once we identified the key criteria and their related documents governing USSOCOM’s SCRM process, we compared the requirements outlined in those documents to procurement documents for specialized equipment manufactured for USSOCOM in calendar years 2018, 2019, and 2020. Our sample consisted of 43 unique Procurement Instrument Identifiers (PIID) for USSOCOM specialized equipment acquisitions for our chosen scope.¹⁰

U.S. Special Operations Command Specialized Equipment Universe and Sample

To evaluate the implementation of the USSOCOM supply chain risk management procedures, we requested that USSOCOM provide the list of specialized equipment acquisitions for four of the nine PEOs included in our evaluation (Command, Control, Communications, and Computers; Maritime; Special Reconnaissance, Surveillance, and Exploitation; and Special Operations Forces Digital Applications) for calendar years 2018, 2019, and 2020. We selected these PEOs based on our assessment of the high quantity of specialized equipment procurements made within the PEOs.

¹⁰ The Federal Acquisitions Regulation, parts 4.1601(A) and 4.1603, state that PIIDs identify specific Government contract instruments. PIIDs consist of a sequence of numbers that indicate: 1) the agency or element issuing the contract instrument, 2) the fiscal year the instrument was awarded or issued, 3) the type of instrument, and 4) the sequence number of the instrument.

USSOCOM provided a universe of 2,412 PIIDs that included dollars obligated, unique identification numbers, and contracting divisions, among other data elements, for each PIID. We identified a non-statistical sample of 49 PIIDs with dollar obligation amounts that exceeded \$7 million. We removed six of these PIIDs because they were duplicates, resulting in 43 unique PIIDs for review. We reviewed the sample of 43 PIIDs to ensure that it contained acquisitions from the contract divisions representing each of the PEOs included in our evaluation.

USSOCOM Supply Chain Risk Management Procedures Did Not Comply With DoD Instructions and Policies

USSOCOM issued a revised supply chain risk management policy in November 2020 that meets DoD requirements, which included making PPPs and PPIPs mandatory for USSOCOM acquisitions. However, SOF AT&L officials do not have a plan to develop PPPs and PPIPs for contracts awarded prior to the issuance of SOF AT&L Policy 70-1.

DoDIs 5000.02T and 5200.39, along with the 2011 PDUSD(AT&L) memorandum, require that DoD personnel complete PPPs as part of all acquisitions. Specifically, these instructions require that all DoD entities use PPPs to establish SCRM responsibilities and include PPPs in all acquisition programs. However, USSOCOM did not require PPPs in its program acquisitions until November 2020. For example, USSOCOM Directive 70-1, established in March 2018, identified PPPs as discretionary. USSOCOM did not provide PPPs for 26 of the 43 specialized equipment acquisitions we reviewed. USSOCOM officials stated that the reason for the missing PPPs was due to USSOCOM Directive 70-1 not requiring PPPs as part of the acquisition process.

The 2011 PDUSD(AT&L) memorandum also requires DoD personnel to ensure contractors have PPIPs in place to protect information critical to the supply chain. However, when we requested PPIPs for the 43 specialized acquisitions in our sample, USSOCOM officials could not provide them. Additionally, USSOCOM officials stated that they would not be able to provide any PPIPs for acquisitions made prior to the November 2020 revision of USSOCOM Directive 70-1. Without PPIPs for contracts awarded prior to the November 2020 revision of USSOCOM Directive 70-1, USSOCOM could not demonstrate how contractors are addressing security concerns that could adversely affect the supply chain.

In November 2020, USSOCOM revised its Directive 70-1 and renamed it “SOF AT&L Policy 70-1.” The revised policy identifies PPPs as mandatory documents and mandates that contractors create PPIPs to address threats listed in the PPP. However, SOF AT&L officials do not have a plan to develop PPPs and PPIPs for acquisitions made prior to the issuance of SOF AT&L Policy 70-1.

USSOCOM Updated Policy to Require PPPs but Has Not Developed PPPs for All of Its Acquisitions

Although the USSOCOM updated its acquisition policy 70-1 in November 2020 to mandate PPPs for all acquisitions, USSOCOM personnel do not have a plan for developing PPPs for active contracts without one. We asked USSOCOM officials for their plan and timelines to create PPPs for all their programs as required by the revised SOF AT&L Policy 70-1. USSOCOM officials replied that they had developed a SOF AT&L Risk Management and Internal Controls Plan in April 2021 that directs SOF AT&L leadership to review acquisition documents on a quarterly basis. The quarterly management reviews and the Mission Tasking Letter address USSOCOM’s effort to ensure PPPs are included in each USSOCOM acquisition.

Not having PPPs in place for all acquisitions introduces significant risk to USSOCOM’s ability to identify, assess, and mitigate supply chain risk. From a universe of 2,412 contract PIIDs, we requested PPPs for the 43 PIIDs we considered significant based on a variety of factors, including cost, complexity of the system, and relevance to combat operations. USSOCOM was not able to provide PPPs for 26 of the 43 PIIDs. DoD program managers develop PPPs to identify and mitigate supply chain risks such as foreign influence, system design vulnerability, or supply chain exploitation. By not developing PPPs, USSOCOM program managers are putting \$541 million of specialized equipment at higher risk of foreign influence, system design vulnerability, or supply chain exploitation.

USSOCOM Updated Policy to Require PPIPs but Has Not Addressed Ongoing Contracts

USSOCOM Directive 70-1 states that a PPIP is a contractor’s plan of how they will protect the information outlined in the PPP, such as supply chain vulnerabilities. Additionally, according to USSOCOM officials, contractors should include details in their PPIPs, such as information vulnerabilities and actions the contractor will take to address these vulnerabilities. We asked USSOCOM officials if they could provide PPIPs for the 43 selected PIIDs. USSOCOM officials stated that they did not make PPIPs a requirement until November 2020, even though, according to the 2011 PDUSD(AT&L) memorandum, PPIPs are an integral part of PPPs. Additionally, USSOCOM officials stated it was unlikely that its PEOs would have any PPIPs prior to FY 2021.

PPIPs ensure that contractors explain how they will address supply chain risks, identified by DoD-developed PPPs, in their project proposals. The USSOCOM contractors that do not have PPIPs in place may not have addressed security concerns that would adversely affect the supply chain.

USSOCOM Did Not Implement Supply Chain Risk Management Procedures in Accordance with DoD Policy

USSOCOM did not implement supply chain risk management procedures in accordance with DoD policy. As a result, USSOCOM did not fully identify, assess, and mitigate supply chain risk during the acquisition and development of USSOCOM specialized equipment. The potential impacts of unidentified supply chain risks include compromised equipment, the inability to identify intellectual property theft, and possible introduction of counterfeit parts into equipment.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Commander of U.S. Special Operations Command, Special Operations Forces Acquisition, Technology, and Logistics Center:

- a. Identify which acquisitions made by the nine U.S. Special Operations Command Program Executive Offices do not have Program Protection Plans in place as required by DoD Instruction 5000.02 and DoD Instruction 5000.83.**
- b. Develop a plan, based on level of risk, to create and implement Program Protection Plans for all Procurement Instrument Identifiers that do not have one in place.**

U.S. Special Operations Forces Acquisition, Technology, and Logistics Center Comments

The Deputy Director for Acquisition, responding for the Commander of U.S. Special Operations Forces Acquisition, Technology, and Logistics Center, agreed with the recommendation. Additionally, the Deputy Director for Acquisition stated that USSOCOM SOF AT&L began an effort on December 20, 2020, to confirm that all programs have a PPP in place by September 30, 2022.

Our Response

The Deputy Director for Acquisition addressed all specifics of the recommendation, and USSOCOM SOF AT&L personnel provided documentation outlining a plan based on a risk analysis that requires the AT&L Director of Acquisition Security to collaborate with program representatives to ensure PPPs for each program of record are current and on file. USSOCOM SOF AT&L stated that programmatic PPPs would address all PPIDs under each program. This documentation fully addressed our recommendation; therefore, recommendations 1.a and 1.b are closed.

Recommendation 2

We recommend that the Commander of U.S. Special Operations Command, Special Operations Forces Acquisition, Technology, and Logistics Center:

- a. Conduct a risk assessment outlining the impact of not having Program Protection Implementation Plans in place prior to November 2020.**
- b. Conduct a cost benefit analysis on the feasibility of requesting that contractors develop Program Protection Implementation Plans for acquisitions that do not have Program Protection Implementation Plans.**
- c. Develop a plan to prioritize the development of Program Protection Implementation Plans based on the level of risk.**

U.S. Special Operations Forces Acquisition, Technology, and Logistics Center Comments

The Deputy Director for Acquisition, responding for the Commander of U.S. Special Operations Forces Acquisition, Technology, and Logistics Center, agreed with the recommendation and stated that USSOCOM SOF AT&L plans to begin a risk assessment on September 1, 2021, with an estimated completion date of April 1, 2022. The Deputy Director for Acquisition also stated that USSOCOM SOF AT&L would subsequently conduct a cost benefit analysis on the feasibility of requesting contractors to develop a PPIP, which will inform a USSOCOM SOF AT&L risk-based prioritized plan for PPIP development.

Our Response

The Deputy Director for Acquisition addressed the specifics of the recommendation; therefore, all parts of the recommendation are resolved, but will remain open. We will close the recommendation once we verify that the USSOCOM SOF AT&L risk assessment outlines the impact of not having PPIPs in place. Additionally, to close this recommendation, we will verify whether USSOCOM SOF AT&L has conducted a cost benefit analysis and has used the analysis to develop a risk-based prioritized plan for PPIP development.

Management Comments

U.S Special Operations Command Special Operations Forces Acquisition, Technology, and Logistics Center



UNITED STATES SPECIAL OPERATIONS COMMAND

7701 TAMPA POINT BOULEVARD
MACDILL AIR FORCE BASE, FLORIDA 33621-5323

SOF AT&L-DC

AUG 24 2021

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL U.S.
DEPARTMENT OF DEFENSE, 4800 MARK CENTER DRIVE, ALEXANDRIA, VA 22350-1500

SUBJECT: Evaluation of United States Special Operations Command's Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment (Project No. D2021-DEVOPD-0052.000)

1. REFERENCE: Draft Report, Department of Defense Inspector General Project D 2021-DEVOPD-0052.000" dated 4 August 2021

2. United States Special Operations Command (USSOCOM) Special Operations Forces Acquisition, Technology and Logistics (SOF AT&L) concurs with the overall findings identified in the report. However, we request the statement "USSOCOM officials do not have a formal plan or detailed guidance to review active contracts to ensure each acquisition has an adequate Program Protection Plan (PPP) in place" be deleted. SOF AT&L has a plan in place, tracks, and requires all programs to develop a PPP.

3. USSOCOM SOF AT&L agrees with the recommendations.

a. Recommendation 1: Started 20 December 2020. Use of the Milestone Document Identification tool to confirm all programs have a PPP in place. Planned completion: Continuous quarterly reviews for status tracking; all programs have PPPs by 30 September 2022.

b. Recommendation 2: Start: 1 September 2021. Planned Completion: 1 April 2022. SOF AT&L will conduct a risk assessment of the impact(s) associated with not having a PPP prior to November 2020. Subsequently, conduct a cost benefit analysis on the feasibility of requesting contractors to develop a Program Protection Implementation Plan (PPIP). Furthermore, that analysis will inform a SOF AT&L risk-based prioritized plan for PPIP development.

4. Point of contact is [REDACTED]

A handwritten signature in black ink, appearing to read "W. Innes".

WILLIAM J. INNES
Deputy Director for Acquisition

Acronyms and Abbreviations

AT&L	Acquisition, Technology, and Logistics
DoDI	Department of Defense Instruction
PDUSD(AT&L)	Principal Deputy Undersecretary of Defense for Acquisition, Technology, and Logistics
PIID	Procurement Instrument Identifier
PPIP	Program Protection Implementation Plan
PPP	Program Protection Plan
SCRM	Supply Chain Risk Management
SOF AT&L	Special Operations Forces Acquisition, Technology, and Logistics
USSOCOM	U.S. Special Operations Command



Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison

703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists

www.dodig.mil/Mailing-Lists/

Twitter

www.twitter.com/DoD_IG

DoD Hotline

www.dodig.mil/hotline



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

