

CUI

INSPECTOR GENERAL

U.S. Department of Defense

JANUARY 12, 2023



(U) Evaluation of Cybersecurity Controls on the DoD's Secure Unclassified Network

Controlled by: DoD OIG
Controlled by: Evaluations
CUI Category: PRIVILEGE, DCRIT, and OPSEC
Distribution/Dissemination Control: FEDCON
POC: Deputy Inspector General for Evaluations, [REDACTED]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

CUI





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

January 12, 2023

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY
 UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
 CHIEF FINANCIAL OFFICER, DOD
 UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY
 ASSISTANT SECRETARY OF DEFENSE (SPECIAL OPERATIONS
 AND LOW-INTENSITY CONFLICT)
 AUDITOR GENERAL, DEPARTMENT OF THE ARMY

(U) SUBJECT: Evaluation of Cybersecurity Controls on the DoD's Secure Unclassified Network
 (Report No. DODIG-2023-044)

(U) This final report provides the results of the DoD Office of Inspector General's evaluation. We coordinated a draft of this report and the proposed recommendations with officials from the offices of the Under Secretary of Defense (Comptroller), the Irregular Warfare Technical Support Directorate (IWTSD) within the Office of the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), the Army Contracting Command (ACC), and the Army Research Lab (ARL). We considered comments from the IWTSD, ACC, and ARL on the draft report, as well as actions taken and documentation provided, when preparing the final report. These comments are included in the report.

(U) We did not receive comments on the draft report from the Under Secretary Of Defense (Comptroller)/Chief Financial Officer. We request that the Under Secretary provide comments on the final report within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendation.

(U) This report contains three recommendations that are considered resolved but remain open and one recommendation that is considered unresolved. As described in the Recommendations, Management Comments, and Our Response section of this report, we will consider the recommendations closed when we have reviewed documentation supporting the actions taken or recommended. We will track these recommendations until an agreement is reached on the actions taken to address the recommendation and when we have received and reviewed adequate documentation showing that all agreed-upon actions are completed.

Controlled by: DoD OIG
Controlled by: Evaluations
CUI Category: ~~PRIVILEGE, DCRIT, and OPSEC~~
Distribution/Dissemination Control: ~~FEDCON~~
POC: Deputy Inspector General for
Evaluations, [REDACTED]

~~(CUI)~~ DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. Send your response to [REDACTED]

~~(CUI)~~ If you have any questions or would like to meet to discuss the evaluation, please contact [REDACTED] We appreciate the cooperation and assistance received during the evaluation.



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

(U) Executive Summary

~~(CUI)~~ We determined that the Irregular Warfare Technical Support Directorate (IWTSD) reviewed and assessed the DoD's Secure Unclassified Network (SUNet) cybersecurity controls, in accordance with the Risk Management Framework (RMF) requirements and the Authority to Operate (ATO) renewal process. However, the IWTSD was unable to directly monitor and manage the execution of cybersecurity and information activities, [REDACTED]

~~(CUI)~~ We found that the IWTSD, which is under the Assistant Secretary of Defense (Special Operations/Low-Intensity Conflict), [REDACTED]

[REDACTED] was the responsibility of the contracting officer's representative (COR), which was staffed by the Army Research Laboratory (ARL). The IWTSD and ARL are not in the same chain of command. Furthermore, the performance work statement (PWS) outlined and defined the ATO renewal and enterprise cybersecurity requirements; however, the PWS combined enterprise and enclave requirements, and neither were expressly prioritized in the PWS.

~~(CUI)~~ Additionally, we found that SUNet did not have dedicated programmatic funding to support enterprise requirements and there was no designated entity obligated to fund enterprise requirements. Furthermore, [REDACTED] and relied on just-in-time funding from mission partners to continue operations, which included Coronavirus Aid, Relief, and Economic Security (CARES) Act funds.¹

(U) We made recommendations for the Executive Director of the Army Contracting Command (ACC), Aberdeen Proving Ground, Adelphi Contracting Division, along with the requiring activities, to conduct a review of the PWS to determine whether it should be revised; to clarify how enterprise funding needs are determined and applied to SUNet; and to determine whether a representative from the IWTSD should serve as an assistant or alternate COR on the SUNet infrastructure contract.

(U) After reviewing management comments, we revised and redirected one recommendation. Three recommendations, made to the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), the Director of the ARL, and the Executive Director of the ACC, are resolved but open. We will close these recommendations when we receive and review supporting documentation for actions taken and the results of the planned reviews. The Under Secretary of Defense (Comptroller)/Chief Financial Officer did not respond to the recommendation made to that office in the report. Therefore, the recommendation is unresolved. We request that the Under Secretary provide comments on the final report.

¹ (U) Public Law 116–136, “Coronavirus Aid, Relief, and Economic Security (CARES) Act,” March 27, 2020.

(U) Objective

(U) The objective of this evaluation was to determine whether the DoD developed, implemented, maintained, and updated security and governance controls to protect the Secure Unclassified Network (SUNet), and the data and technologies that reside on it, from internal and external threats.

(U) Background

(~~CUI~~) SUNet is a secure unclassified DoD system that [REDACTED] [REDACTED] The Irregular Warfare Technical Support Directorate (IWTSD), under the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), developed SUNet to address the DoD's need for a secure unclassified information platform to support rapid innovation; research, development, testing, and evaluation; combined operational missions; and information sharing between mission partners. Although the IWTSD owns and accredits SUNet, a private contractor manages the system.

(~~CUI~~) SUNet allows the DoD, other U.S. Government agencies, and their partners, including academia, research, and foreign partners, to communicate, share, analyze, and disseminate information in near-real-time. SUNet supports more than a dozen [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Cybersecurity Risk Management, SUNet Accreditation, and Authority to Operate

(U) SUNet employs an assessment and authorization process, in accordance with DoD Instruction 8510.01, to address all matters related to the DoD's implementation of the information technology Risk Management Framework (RMF).³

³ (U) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Systems," July 19, 2022.

(U) Risk Management Framework and Cybersecurity Controls

(U) The RMF provides cybersecurity requirements for DoD information technologies, consistent with the principles established by the National Institute for Standards and Technology (NIST).⁴ The RMF is an integrated DoD enterprise-wide decision structure for cybersecurity risk management and implements a multi-faceted approach to cybersecurity risk management, developed by the NIST.⁵ The RMF provides a flexible approach to effectively manage security and privacy risks for information technology systems and networks. The RMF has six steps:

- (U) categorize the system,
- (U) select security controls,
- (U) implement security controls,
- (U) assess security controls,
- (U) authorize the system, and
- (U) monitor security controls.

(U) The RMF categorizes information systems based on the impact of the potential loss of confidentiality, integrity, and availability of information processed, stored, and transmitted on the system. The resulting low, moderate, or high system categorization determines the cybersecurity requirements and controls that should be implemented. Cybersecurity controls are defined and cataloged by NIST and are implemented and assessed by system owners consistent with NIST assessment principles.⁶ SUNet operates at a moderate security categorization, and the specific controls implemented on SUNet are prescribed by the security categorization outlined in NIST 800-53A.

(U) The DoD uses the web-based Enterprise Mission Assurance Support Service (eMASS), which automates a broad range of processes related to cybersecurity management and RMF assessment and authorization. The DoD also uses eMASS to track and record security authorization packages, which are the mechanisms for obtaining authority to operate (ATO) decisions.

(U) Once the system owner registers and categorizes a system, such as SUNet, in eMASS, eMASS automatically applies baseline cybersecurity controls that correspond to the system's security categorization. The system owner may add controls to increase the system's security posture. The result of this process is a set of security controls tailored to specific system

⁴ (U) NIST Special Publication 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," (December 2018).

⁵ (U) DoDI 8510.01.

⁶ (U) NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," December 10, 2020, and NIST Special Publication 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations," January 2022.

(U) vulnerabilities, security categorization, and accepted risk tolerance. The system owner documents the final security control set, along with the supporting rationale for control selection, in the system security plan.

(U) Authority to Operate and Authorizing Official

(U) In accordance with DoD Instruction 8510.01, each DoD information system, DoD partnered system, and platform information technology system must have an authorizing official responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture. The ATO is the official management decision given by a senior Federal official, or officials, to authorize the operation of an information system and explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.⁷ The IWTSD International Program Manager, a senior executive, serves as the authorizing official for SUNet.

(U) To support the authorizing official's RMF review process and authorization decision, the IWTSD appointed additional personnel to serve as:

- (U) security controls assessor (SCA),
- (U) information system security managers, and
- (U) information systems security officers.

(CUI) [REDACTED]

(U) SUNet System Structure

(CUI) [REDACTED]

The SUNet system consists of the enterprise and multiple enclaves within the system.

⁷ (U) Committee On National Security Systems, "Committee On National Security Systems (CNSS) Glossary," CNSSI-4009, March 2, 2022.

(U) SUNet Enterprise

(U) The SUNet enterprise is the core infrastructure that houses the overall system requirements and the baseline infrastructure in which the enclaves reside. SUNet enterprise services and requirements include activities such as:

- (U) domain authentication,
- (U) scanning and monitoring,
- (U) security configuration,
- (U) firewall management,
- (U) management of all connections to SUNet,
- (U) server maintenance,
- (U) patching, and
- (U) multi-factor authentication.

~~(CUI)~~ All mission partner enclaves are consumers of SUNet enterprise services and are entitled to several SUNet enterprise baseline services, some of which are mandatory.

[REDACTED]

(U) SUNet Enclaves

~~(CUI)~~ [REDACTED]

(U) How SUNet Is Funded

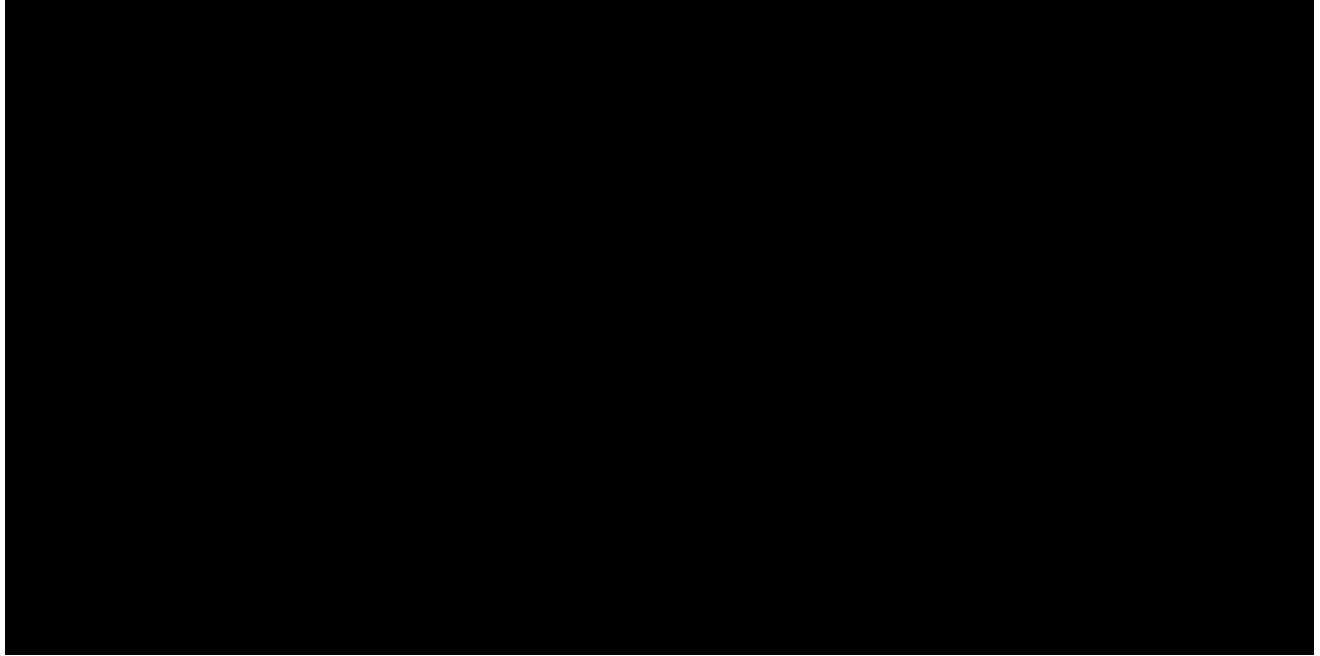
(U) The SUNet infrastructure contract includes both SUNet enterprise and enclave requirements.⁸ In addition, some enclave mission partners have their own, separate contracts for enclave activities and support.

~~(CUI)~~ The SUNet infrastructure contract incorporated [REDACTED]

⁸ ~~(CUI)~~ [REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(U) Figure 1. SUNet Fee Structure



(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]

(U) The SUNet Infrastructure Contract

~~(U)~~ The IWTSD partnered with the ARL to gather system requirements and solicit proposals for SUNet. [REDACTED]

[REDACTED] The cost-plus fixed fee contract contains multiple contract line item numbers that are assigned to SUNet [REDACTED]

[REDACTED] The funding associated with the contract line item numbers include operation and maintenance funds and research and development funds. The SUNet infrastructure contract was incrementally funded, but the contract was never fully funded nor has the contract ceiling been met or exceeded. Funding allocated to the contract aligned to the cost estimates provided by the contractor, and funding was allotted to the contract for designated performance periods. The contract line item numbers state that the contractor will perform SUNet infrastructure services in accordance with the contract performance work statement (PWS).

(U) Performance Work Statement

(U) The Federal Acquisition Regulation outlines the elements of a PWS, which describes the required results of the contract, establishes measureable performance standards, and relies on those standards and financial incentives in a competitive environment to encourage competitors to develop and institute innovative and cost-effective methods of performing the work.¹⁰ The PWS is incorporated into the final contract award and is adopted at the start of a contract. Personnel from the ARL, with input from the IWTSD, wrote the PWS for the SUNet infrastructure contract. The PWS covers the SUNet system and contains both SUNet enterprise requirements and enclave requirements.

(U) SUNet Infrastructure Contract Management Roles and Responsibilities

(U) The primary roles that support contract administration and monitoring include the contracting officer, the contracting officer's representative (COR), and the technical monitor (TM). For the SUNet infrastructure contracts, personnel from several DoD entities fulfilled these roles.

¹⁰ [REDACTED]
 (U) Federal Acquisition Regulation Part 37, "Service Contracting," Subpart 37.602, "Performance Work Statement."

(U) Army Contracting Command–Contracting Officer

(U) The ACC is a subordinate command of the Army Materiel Command. The ACC-Aberdeen Proving Ground Contracting Center is responsible for acquiring quality, technologically superior, next-generation equipment and services in the shortest time, while obtaining best value. The ACC–Aberdeen Proving Ground Contracting Center is a full service, life-cycle acquisition organization.

(U) ACC–Aberdeen Proving Ground Contracting Center personnel serve as the contracting officer for the SUNet infrastructure contract. The contracting officer is responsible for ensuring compliance with the terms of the contract and ensuring that performance requirements are met. The duties of the contracting officer include ensuring that contractors receive impartial, fair, and equitable treatment; appointing a COR; and assigning responsibilities to the COR. The contracting officer can request the advice of specialists in audit, law, engineering, information security, and other fields, as appropriate, to assist in performance monitoring.

(U) Army Research Laboratory–Contracting Officer’s Representative

(U) The U.S. Army Combat Capabilities Development Command Army Research Laboratory (ARL) is the Army’s national research laboratory and is part of the Army Futures Command. The ARL focuses on cutting-edge scientific discovery, technological innovation, and transition of knowledge from commercial partners to DoD personnel.

(U) The team lead of the ARL Concept Development Team, Technology Integration Branch, serves as the COR for the SUNet infrastructure contract. The COR’s primary responsibility is managing the day-to-day operations and monitoring the progress of the contract by directly engaging with the contractor. The COR must be a Federal employee, be appointed in writing, complete required training, and, in some cases, meet specific experience requirements if the contract requires specialized knowledge.

(U) Technical Monitors

(U) The contracting officer may also appoint a TM to assist in monitoring contractor performance, if the COR requires additional support. The TM, similar to a COR, is appointed in writing and is required to complete training requirements. The TM provides reports on contractor performance for the COR’s review. For the SUNet infrastructure contract, personnel from more than a dozen mission partners serve as TMs to monitor their designated enclaves, as well as an enterprise TM from the IWTSD.

(U) Finding

(U) The IWTSD Reviewed and Assessed SUNet Cybersecurity Controls, but Was Unable to Monitor and Manage the Execution of Cybersecurity Activities

(U) The IWTSD reviewed and assessed SUNet cybersecurity controls in accordance with RMF requirements and the ATO renewal process. However, the IWTSD was unable to directly monitor, manage, or prioritize the execution of SUNet cybersecurity and information activities.

~~(CUI)~~ In part, this occurred because the SUNet infrastructure contract PWS outlined and defined the ATO renewal and enterprise cybersecurity requirements; however, the PWS combined enterprise and enclave requirements, and neither were expressly prioritized in the PWS. [REDACTED]

(U) In addition, SUNet did not have dedicated programmatic funding to support enterprise requirements, and there was no designated entity obligated to fund enterprise requirements or budget shortfalls. Instead, SUNet relied on just-in-time funding from mission partners to continue operations. Furthermore, the contractor-designed funding model did not fully cover enterprise requirements or costs.

~~(CUI)~~ The inability to prioritize cybersecurity activities, lack of direct monitoring, and funding shortfalls [REDACTED]

Without secure funding for the enterprise requirements and full support for ATO requirements and maintenance, SUNet and the mission-essential activities that are enabled by SUNet are at risk of termination due to non-compliance with cybersecurity requirements.

(U) The IWTSD Reviewed and Assessed SUNet Cybersecurity Controls

(U) The IWTSD reviewed and assessed SUNet cybersecurity controls in accordance with RMF requirements and the ATO renewal process. The security controls assessor reviewed and assessed each of SUNet's more than 400 security controls. The assessor examined and tested each control to determine whether the control was planned and implemented correctly, operated as needed, and produced the desired results based on the RMF. The assessor also interviewed the SUNet team members responsible for implementing the security controls and provided feedback and recommendations for the remediation of gaps to help the team identify supporting documentation and to enable the assessor to approve the security controls in

(U) eMASS. Any controls the assessor determined to be noncompliant required the SUNet team to create a plan of action and milestone document and upload the document to eMASS for review and approval in accordance with NIST Special Publications 800-37 and 800-53.¹¹

(U) For example, during the security control assessment, the assessor examined, interviewed, and tested a specific security control that displayed a warning banner on the SUNet virtual private network landing page before a user logged into the SUNet environment. After reviewing the implementation of this security control across SUNet, the assessor found that the control was noncompliant because the warning banner did not display consistently. To mitigate and remediate the noncompliant control, the SUNet team responsible for implementing the control created a plan of action and milestone and uploaded it to eMASS to document the status and path to compliance for the control.

(U) In addition, during the 2022 ATO renewal process, the IWTSD assessor reviewed all of the more than 400 SUNet security controls in eMASS, in accordance with NIST Special Publication 800-53A, DoD policies, and SUNet policies and procedures. During the ATO renewal process, the IWTSD assessor was in constant communication with the SUNet teams responsible for implementing the security controls and providing the supporting documentation in eMASS. The IWTSD assessor analyzed and created post-assessment reports, including the risk assessment report, security assessment results, and plans of action and milestones. The assessor also submitted the complete ATO renewal package to the authorizing official for review and authorization.

(U) The IWTSD Had Limited Ability to Prioritize and Manage the Implementation of Cybersecurity Requirements

~~(CUI)~~ The SUNet infrastructure contract PWS outlined and defined the ATO renewal and enterprise cybersecurity requirements; however, the PWS combined enterprise and enclave requirements, and neither were expressly prioritized in the PWS. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) The SUNet PWS Did Not Prioritize Requirements

(U) The SUNet PWS combined enterprise and enclave requirements. Specifically, the PWS outlined and defined cybersecurity requirements and the requirement to maintain an ATO, as well as requirements to develop and deploy enclaves to SUNet.

¹¹ (U) NIST Special Publication 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," (December 2018) and NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," December 10, 2020.

(U) For example, the SUNet PWS stated that the contractor must ensure that SUNet is protected and accredited in accordance with applicable guidelines and maintain the ATO throughout the period of performance for the SUNet effort. The PWS also stated:

(cui) _____

(CUI) ARL personnel, with input from the IWTSD, wrote the PWS for the SUNet infrastructure contract. Though the PWS did include stipulations to maintain an ATO for SUNet throughout the period of performance, it did not prioritize this requirement in any way. Nor did the contract, the PWS, or the quality assurance surveillance plan prioritize the ATO. [REDACTED]

[REDACTED]

(U) The IWTSD Had Limited Ability to Ensure That the Contractor Prioritized Cybersecurity Activities

(CUI) [REDACTED]

The IWTSD SUNet Program Manager served as the TM for the enterprise; however, the Program Manager was one of more than a dozen TMs reporting and providing feedback to the ARL COR.

(U) The ARL COR stated that she monitored contractor performance and adhered to the PWS and quality assurance surveillance plan associated with the infrastructure contract. In addition, the COR stated that she did not prioritize any TM's information and reporting over another's. Additionally, ARL officials stated that they believed that rather than advocating for the prioritization of enterprise requirements, the IWTSD, as the SUNet system owner and generator of enterprise requirements, should fund the enterprise requirements. However, IWTSD officials stated that the enterprise requirements were driven by Government standards

¹² (U) SUNet Performance Work Statement, Section C.3, "Requirements," Subsection C.3.2, "Systems Integration Plan," Requirement C.3.2.2.

¹³ (U) A zero-day attack is a cyberattack that exploits a previously unknown hardware, firmware, or software vulnerability.

(U) and the contractor generated the cost estimates in response to all enterprise and enclave requirements. IWTSD officials believed the cost estimates generated by the contractor did not sufficiently align to requirements.

(U) Furthermore, neither the ARL COR nor the IWTSD TM could clearly explain how the cost-recovery enterprise fee and fee-for-service “enclave tax” were being applied to enterprise requirements. The COR stated that even though she reviewed invoices monthly, after they were paid by the administrative contracting officer, she was unable to map the invoices to accounting data that clearly showed how the money was allocated to enterprise or enclaves. The only indicator of how the funding was allocated were the contractor-determined charge codes listed on the invoices. In addition, the IWTSD TM, who was the SUNet Program Manager, expressed concerns in TM reports to the COR, in correspondence with the contracting agencies, and to the DoD OIG evaluation team, about their inability to understand how the funding model created by the contractor aligned to the execution of enterprise requirements.

~~(CUI)~~ [REDACTED]
[REDACTED]
[REDACTED] In addition, the contractor notified the Government on multiple occasions that it did not have enough resources to [REDACTED] The only mechanism available to the IWTSD to prioritize cybersecurity requirements was to suspend the SUNet Change Control Board.¹⁴ This action paused all non-cybersecurity-related tasks and halted all enclave mission support activities to focus contractor resources on cybersecurity requirements, which [REDACTED] However, suspending the Change Control Board was the IWTSD’s only available action to shift focus and compel the contractor to pause non-essential work.

~~(CUI)~~ For example, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

(CUI) Lack of Programmatic Funding and a Complex Funding Structure

(CUI) SUNet did not have dedicated programmatic funding to support enterprise requirements, and there was no designated entity obligated to fund enterprise requirements or budget shortfalls. Instead, SUNet relied on just-in-time funding from mission partners to continue operations. [REDACTED]

(U) SUNet Lacked Programmatic Funding

(U) Though the IWTSD historically contributed funding to the SUNet infrastructure contract, the IWTSD is not a program office and is not resourced or obligated to fully fund SUNet. However, as SUNet grew and oversight requirements increased, the IWTSD redirected internal funding and sought additional funding to hire personnel to support the oversight and execution of SUNet cybersecurity needs and ATO renewal review; respond to taskings from the U.S. Cyber Command on behalf of SUNet; and build out a Security Operations Center to improve the IWTSD's ability to track and respond to cybersecurity threats and incidents. The IWTSD took these steps [REDACTED] and to better position the IWTSD and SUNet to respond to increased complexity and oversight.

(U) Complex Funding Structure Did Not Fully Cover Costs of SUNet Enterprise Requirements

[illegible]

(U) In FY 2021, the Under Secretary of Defense for Intelligence and Security provided \$2 million in CARES Act funding to maintain SUNet operations as SUNet enclaves were hosting DoD COVID-19 operational support activities and continued SUNet operations were at risk. This evaluation did not review whether the CARES Act funding provided to SUNet was in accordance with the guidance issued by the Office of Management and Budget and the Office of the Under Secretary of Defense (Comptroller) and the purpose statute; however, CARES Act guidance issued by the offices requires that officials use CARES Act funds to prevent, prepare for, and respond to the COVID-19 pandemic.¹⁵ The guidance further states that officials must maintain evidence that clearly articulates the need for goods and services acquired using CARES Act funding. A purpose statute violation may lead to an Antideficiency Act violation if there are not enough funds available from the proper appropriation to pay for the purchases. The Antideficiency Act prohibits agencies' officials from making or authorizing an expenditure in excess of amounts of funds appropriated.¹⁶ A review of this transaction could result in the potential monetary benefits of up to \$2 million in questioned costs.

(~~CUI~~) The Government has an obligation, created by the contract, to fund the requirements outlined in the contract. However, for the SUNet infrastructure contract, the Government did not fully fund the contract because there was no program office or entity obligated to fund it

[REDACTED] For example, according to documentation provided by the ARL, in [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] assumed that all enclave owners paid their enterprise services fee.

(~~CUI~~) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹⁵ (U) Section 1301(a), title 31, United States Code (31 U.S.C. § 1301(a))—also referred to as the purpose statute—states that public funds may be used only for the purpose or purposes for which they were appropriated.

¹⁶ (U) 31 U.S.C. § 1341(a)(1)(A).

(CUI) Without Prioritized Cybersecurity Requirements and Dedicated Program Funding, [REDACTED]

(CUI) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(CUI) Additionally, without designated enterprise funding, or aligning enterprise funding to system-wide enterprise PWS requirements, [REDACTED]
[REDACTED] For example, SUNet's current ATO is conditional and requires vigilance and strict adherence to enterprise requirements.
[REDACTED]
[REDACTED]
[REDACTED]

(U) Management Comments on the Finding

(U) Army Research Laboratory Comments

(U) In addition to responding to the recommendations, the ARL Director provided comments on the Finding. For the full text of the Director's comments, see the Management Comments section of the report.

(U) The ARL Director disagreed with our finding that the IWTSD was unable to directly monitor and manage the execution of cybersecurity and information activities because direct monitoring of contractor performance was the responsibility of the COR. The Director stated that as a TM on the contract, the IWTSD was directly empowered to monitor contractor performance and that the IWTSD did direct activities via the Change Control Board. The Director also disagreed with the finding that SUNet did not have programmatic funding.

(U) Our Response

(CUI) As we note in the Finding, the IWTSD TM is one of many TMs providing feedback to the COR, and the COR did not prioritize the IWTSD's reports and feedback. We reviewed multiple reports from the IWTSD TM to the COR that noted concerns with the contractor's performance related [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Additionally, as we state in the report, [REDACTED]
[REDACTED]
[REDACTED]

The Change Control Board is a reviewing body, not

(~~CUI~~) an enforcement body and did not enable any additional direct oversight, monitoring, or management of cybersecurity activities. Rather, the IWTSD suspended the Change Control Board to effectively [REDACTED]
[REDACTED]

(~~CUI~~) Although the ARL Director stated that the IWTSD was funded and directed by Congress to manage and maintain SUNet, we did not find any corresponding direction from Congress to the Under Secretary of Defense for Policy, the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), or the IWTSD. The document provided by the ARL Director is an excerpt from a budget request, not a funding appropriation or authorization and does not direct or state that the funding requested or received will be applied to the infrastructure contract. Furthermore, the amount cited, \$4.6 million, would have been insufficient to cover the full enterprise requirements, [REDACTED]

(~~CUI~~) As we noted in the report, SUNet infrastructure is funded by participant contributions and augmented by just-in-time funding. We also highlighted the additional requirements levied by the IWTSD to support SUNet and directly monitor and manage SUNet's cybersecurity and information activities, such as establishing a SUNet Security Operations Center and responding to taskings from the U.S. Cyber Command. We determined that there is no single entity obligated to fund SUNet's enterprise requirements and call attention to this [REDACTED]
[REDACTED]

(U) We reviewed the ARL Director's comments to the finding, but we did not amend our Finding as a result of the comments or documentation provided.

(U) Recommendations, Management Comments, and Our Response

(U) Redirected Recommendations

(U) As a result of management comments, we redirected Recommendations 1.a and 1.b to the Director of the Army Research Laboratory, which has the authority to implement the recommendations. In addition, we renumbered draft Recommendations 1.c, 2, and 3 as Recommendations 2, 3, and 4.

(U) Recommendation 1

(U) We recommend that the Director of the Army Research Laboratory, in conjunction with the Army Contracting Command, Aberdeen Proving Ground, Adelphi Contracting Division:

- a. **(U) Conduct a review of the enterprise requirements and the performance work statement to determine whether the scope of the current contract should be revised to clearly support the Secure Unclassified Network's cybersecurity requirements and authority to operate.**
- b. **(U) Conduct a review to determine how to increase transparency and communication between the Government parties to the contract to clarify how enterprise funding needs are determined and applied to Secure Unclassified Network enterprise requirements; and to ensure that Secure Unclassified Network enterprise requirements are being fully executed as required.**

(U) Army Research Laboratory Comments

(U) The ARL Director agreed with the recommendation and stated that the ARL will complete a review of the requirements, PWS, communications, and oversight of the SUNet enterprise contract by January 16, 2023.

(U) Our Response

(U) The ARL Director's comments addressed the specifics of the recommendation. Therefore, the recommendation is resolved, but remains open. We will close the recommendation when the ARL Director provides us the results and actions taken from the planned review and we verify that the results and actions taken increased transparency and communication on funding for SUNet enterprise requirements.

(U) Recommendation 2

(U) We recommend that the Executive Director of the Army Contracting Command, Aberdeen Proving Ground, Adelphi Contracting Division, in conjunction with the requiring activities, conduct a review to determine whether a representative from the Irregular Warfare Technical Support Directorate, or any future designated Secure Unclassified Network system owner and/or program office that controls SUNet's Authority to Operate, should be the assistant or alternate contracting officer's representative on the SUNet infrastructure contract and any contracts providing services that rely upon SUNet's infrastructure.

(U) Army Contracting Command Comments

(U) The ACC Executive Director agreed with the recommendation and stated that the ACC will coordinate with the ARL to determine whether a representative from the IWTSD should be an assistant or alternate COR on the SUNet infrastructure contract by January 18, 2023.

(U) Our Response

(U) The ACC Executive Director's comments addressed the specifics of the recommendation. Therefore, the recommendation is resolved, but remains open. We will close the recommendation when the ACC Executive Director provides us the results of the review, actions taken, and, as appropriate, letters of appointment for any additional CORs named and if determined additional representatives should be an assistant or alternate COR, copies of their appointment letters.

(U) Recommendation 3

(U) We recommend that the Under Secretary of Defense (Comptroller) review the transaction to determine whether the Office of the Under Secretary of Defense for Intelligence and Security used Coronavirus Aid, Relief, and Economic Security Act funds appropriately; and based on the review, determine whether any purpose statute violations and resulting Antideficiency Act violations exist and, if so, take appropriate action. This review could result in the potential monetary benefits of up to \$2 million in questioned costs.

(U) Management Comments Required

(U) The Under Secretary of Defense (Comptroller)/Chief Financial Officer, did not respond to the recommendation. Therefore, the recommendation is unresolved. We request that the Under Secretary provide comments on the final report.

(U) Recommendation 4

(U) We recommend that the Under Secretary of Defense for Policy, in conjunction with the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict), conduct a review to determine the long-term strategy for the management, resourcing, and oversight of the Secure Unclassified Network.

(U) Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) Comments

~~(CUI)~~ The Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) agreed with the Finding and recommendation and outlined various steps his office and the IWTSD were taking to address the recommendation. Specifically, these steps included

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Our Response

~~(CUI)~~ Comments from the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) addressed the specifics of the recommendation; therefore, the recommendation is resolved, but open. We will close the recommendation when we obtain and review the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) Scope and Methodology

(U) We conducted this evaluation from February 2022 through August 2022 in accordance with the “Quality Standards for Inspection and Evaluation,” published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met 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.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(U) Interviews with Officials

(U) To complete our evaluation, we conducted teleconferences, interviews, and requests for information from

- (U) Army Contracting Command–Aberdeen Proving Ground, Maryland
- (U) Army Research Laboratory–Adelphi Laboratory Center, Maryland
- (U) Irregular Warfare Technical Support Directorate, Alexandria, Virginia

(U) Documentation Review

~~(CUI)~~ We identified the contract associated with this evaluation, [REDACTED], through a self-initiated followup on the evaluation Report No. DODIG-2022-0049, “Evaluation of Contract Monitoring and Management for Project Maven,” issued January 6, 2022.

(U) To determine whether the DoD developed, implemented, maintained, and updated security and governance controls to protect SUNet, we requested and obtained the following documents:

- (U) PWS for the Infrastructure contract
- (U) TM reports for the Infrastructure contract
- (U) ATO renewal package for SUNet

(U) In addition, we researched, reviewed, and obtained the following criteria documents:

- (U) DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014 (Incorporating Change 1, October 7, 2019)
- (U) DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014 (Incorporating Change 3, December 29, 2020)
- (U) DoD Instruction 8530.01, “Cybersecurity Activities Support to DoD Information Network Operations,” March 7, 2016 (Incorporating Change 1, July 25, 2017)
- (U) NIST Special Publication 800-37, Revision 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018
- (U) NIST Special Publication 800-53, Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” December 10, 2020
- (U) NIST Special Publication 800-53A, Revision 5, “Assessing Security and Privacy Controls in Information Systems and Organizations,” January 2022

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) and the DoD Office of Inspector General (DoD OIG) issued four reports discussing cybersecurity, RMF, and the protection of CUI on contractor-owned networks.

(U) Unrestricted GAO reports can be accessed at <http://www.gao.gov>. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

(U) GAO

(U) Report No. 22-105259, “Defense Cybersecurity: Protecting Controlled Unclassified Information Systems,” May 2022

(U) The GAO determined that the DoD had achieved varied results in implementing four selected cybersecurity requirements for CUI systems, with more progress being made in some of the requirements than with others. These selected requirements included: (1) categorizing the impact of loss of confidentiality, integrity, and availability of individual systems as low, moderate, or high; (2) implementing specific controls based in part on the level of system impact; and (3) authorizing these systems to operate.

(U) DoD OIG

(U) Report No. DODIG-2022-049, “Evaluation of Contract Monitoring and Management of Project Maven,” January 6, 2022

(U) The DoD OIG determined that the Algorithmic Warfare Cross-Functional Team did not document its approach to monitoring Project Maven’s four contracts and that without formalized and documented processes, there was an increased risk of lapses occurring in the monitoring and management of the Project Maven contracts as the program grew and as project personnel changed. Furthermore, the DoD OIG determined that this could have negatively affected the long-term success and growth of the project.

(U) Report No. DODIG-2022-041, “Audit of the DoD’s Use of Cybersecurity Reciprocity Within the Risk Management Framework Process,” December 3, 2021

(U) The DoD OIG determined that the U.S. Transportation Command and the Defense Health Agency leveraged reciprocity to reduce redundant test and assessment efforts while authorizing their systems through the RMF process; but that the Defense Logistics Agency and Defense Human Resources Activity did not.

(U) Report No. DODIG-2019-105, “Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems,” July 23, 2019

(U) The DoD OIG determined that DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information. Furthermore, the DoD OIG determined that DoD Component contracting offices and requiring activities did not always know which contracts required contractors to maintain CUI because the DoD did not implement processes and procedures to track which contractors maintain CUI. In addition, the DoD OIG determined that the contracting offices inconsistently tracked which contractors maintain CUI on their networks and systems.

(U) Potential Monetary Benefits

(U) Recommendation 3 of this report identifies a questioned cost of up to \$2 million. The exact amount will be determined after a review of the transaction by the Office of the Under Secretary of Defense (Comptroller).


(U) Management Comments

(U) Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)

~~CUI~~

INFO MEMO

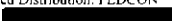
FOR: DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

FROM: Christopher P. Maier, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict 

SUBJECT: Response to the Draft Report, Project No. D2022-DEV0PD-0082.000

References:

- (a) DoD Inspector General Draft Report, "Evaluation of Cybersecurity Controls on the DoD's Secure Unclassified Network, Project No. D2022-DEV0PD-0082.000," November 4, 2022.
- (b) IWTSD Operating Charter, January 4, 2021
- I concur with the Office of Inspector General (OIG) findings and recommendations identified in Reference (a). The Office of Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (ASD SO/LIC) and its Irregular Warfare Technical Support Directorate (IWTSD) reaffirm that the long-term management, oversight, and accreditation of the Secure Unclassified Network (SUNet) system will remain with IWTSD; each element is addressed below.
- **Management.** SUNet is an enduring RDT&E requirement and directly aligns with IWTSD's charter. IWTSD's expertise, as it relates to rapid and iterative development, has become integral to SUNet's agile accreditation and change control processes.
- Actions ongoing:
 - IWTSD is updating a SUNet System Development and Management Plan to codify IWTSD's role as system owner and guiding principles for managing SUNet. Additionally, IWTSD is meeting with all of the SUNet stakeholders and mission partners to discuss requirements and align priorities.
- **Resourcing.** As an enduring system, I agree that funding to sustain the SUNet enterprise should be programmed to IWTSD, the SUNet system owner. This would ensure dedicated funding for enterprise requirements necessary to maintain SUNet's authority to operate and an acceptable cyber security posture.
- Actions ongoing:
 - My organization is reviewing funding requirements and will discuss with the DoD Comptroller and Cost Assessment and Program Evaluation (CAPE) the potential of increasing the ASD(SO/LIC) Advanced Development (PE 0603121D8Z) across the FYDP to ensure dedicated funding for the SUNet system security, development, management, and maintenance.

Controlled by: ASD SO/LIC IWTSD
 CUI Category: PRIVILEGE, DCRIT, OPSEC
 Limited Distribution: FEDCON
 POC: 

~~CUI~~

(U) Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (cont'd)

CUI

- (U) **Oversight.** I agree that IWTSD must have direct oversight of SUNet to ensure it sustains mission critical activities in support of current and future operations. The current contract structure and administration, coupled with the lack of dedicated program funding, limit IWTSD's ability to direct and manage the execution of required cyber security activities and increases risk to SUNet and the critical missions it supports.
- Actions taken:
 - IWTSD recently added five technical staff and established an internal security operations center to detect, analyze, and report threats and incidents in a timely manner to defend and protect networks and the supporting missions within IWTSD's area of operations.
 - IWTSD partnered with General Service Administration (GSA) Federal Systems Integration and Management Center (FEDSIM) to conduct a competitive acquisition prior to the last Period of Performance (PoP) of the existing US Army Research Laboratory (ARL) contract, and GSA FEDSIM has advertised this competitive procurement on its opportunity page. IWTSD and GSA FEDSIM have conducted market assessment discussions with interested vendors and completed the acquisition plan.
- Actions ongoing:
 - IWTSD continues to work with GSA FEDSIM on the competitive procurement and subject to the availability of funding, is on schedule to award the new contract by summer 2023 to allow for full transition of the infrastructure, program management, and information assurance no later than September 2023. The enclaves will transition to the new contract as the mission partners approach their respective renewal cost cycles.

CUI

(U) Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (cont'd)

UNCLASSIFIED

CHARTER OF THE

IRREGULAR WARFARE TECHNICAL SUPPORT DIRECTORATE

OF THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT

Purpose. The purpose of this Charter is to describe the mission and responsibilities of the Irregular Warfare Technical Support Directorate (IWTSD) in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD(SO/LIC)).

Background. The Acting Secretary of Defense on November 18, 2020, authorized the ASD (SO/LIC) to transform the Combating Terrorism Technical Support Office into the Irregular Warfare Technical Support Directorate under the ASD(SO/LIC)'s authority, direction, and control.¹ Accordingly, the Combating Terrorism Technical Support Office (CTTSO) is hereby transformed into the Irregular Warfare Technical Support Directorate (IWTSD), which will operate as a directorate of the Office of the ASD(SO/LIC) under the authority, direction, and control of the ASD(SO/LIC).²

Organization and Purpose. The IWTSD supports the ASD(SO/LIC) in the development of capabilities for the Department of Defense (DoD) to counter and conduct the full spectrum of irregular warfare (IW),³ which includes missions of unconventional warfare (UW), stabilization, foreign internal defense (FID), counterterrorism (CT), and counterinsurgency (COIN).⁴ Consistent with that purpose, the IWTSD will assume the former functions of the CTTSO in international cooperative research and development activities and will continue to develop and implement agreements and task plans with current and future international partners as approved by the ASD(SO/LIC) and in accordance with applicable DoD policy for international agreements.⁵ The CTTSO program

¹ Acting Secretary of Defense Memorandum, "Organizational Role of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict," November 18, 2020.

² See DoD Directive 5111.10, "Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD (SO/LIC))." March 22, 1995 (Incorporating Change 2, October 21, 2011).

³ See Department of Defense Directive 3000.07, "Irregular Warfare," August 28, 2014 (Incorporating Change 1, May 12, 2017).

⁴ Joint Publication 1, Doctrine for the Armed Forces of the United States (2017); Department of Defense, Irregular Warfare: Countering Irregular Threats, Joint Operating Concept Version 2.0 (2010); Department of Defense, Irregular Warfare Annex to the National Defense Strategy (2020).

⁵ DoD has concluded such agreements or arrangements with counterpart ministries of Israel (2005), the United Kingdom (2005), Canada (2009), Australia (2006), and Singapore (2006) pursuant to 10 U.S.C. § 2350a, 10 U.S.C. § 2350b, and 22

UNCLASSIFIED

(U) Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (cont'd)

UNCLASSIFIED

management functions for the Technical Support Working Group (TSWG) will be renamed and incorporated into the IWTSD, as needed.⁶

Mission and Functions. The mission of the IWTSD is to identify and develop capabilities for the Department of Defense (DoD) to conduct IW against all adversaries, including Great Power competitors and non-state actors, and to deliver those capabilities to DoD components and interagency partners through rapid research and development, advanced studies and technical innovation, and provision of support to U.S. military operations.

The IWTSD accomplishes the IW mission in three related lines of effort. First, the IWTSD identifies operational requirements from warfighters, incorporates the policy priorities of the DoD civilian leadership, and rapidly develops and delivers advanced capabilities that improve the capacity of DoD to prepare for and conduct all aspects of IW, including as it relates to Great Power competition, major combat operations, and post-conflict stabilization and transition. Second, the IWTSD works with partner country ministries of defense under bi-lateral agreements or arrangements to conduct cooperative research and development, which allows the U.S. DoD to expand IW capabilities by leveraging foreign experience, expertise, and resources. Third, the IWTSD collaborates with and supports related requirements of non-DoD U.S. Government departments and agencies to understand those users' priorities and requirements, to share expertise, and to develop mutually beneficial capabilities.

Charter. The IWTSD is chartered to support DoD IW activities and objectives, to the extent authorized by statute or otherwise consistent with the purpose of available appropriations, by:

1. Conducting research, development, testing, and evaluation (RDT&E) and information sharing to develop rapidly and fill the capability gaps of the operational community;
2. Providing prototypes for operational testing and evaluation (OT&E) and training and support for the prototypes to DoD components in furtherance of U.S. military operations and to interagency users for operational evaluation and feedback;
3. Procuring commercial or non-developmental items for testing and operational evaluation that relate to RDT&E efforts;⁷

U.S.C. § 2767. DoD Instruction 5530.03, "International Agreements," or successor guidance governs the development, review, negotiation, conclusion, and reporting of additional agreements.

⁶ The CTTSO has exercised program management authority for the TSWG, which has provided an interagency forum for identification, prioritization, and coordination of interagency and international research and development (R&D) requirements for combating terrorism.

⁷ Efforts of this nature may be financed by RDTE, O&M, or Procurement appropriations (as determined in accordance

UNCLASSIFIED

(U) Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict) (cont'd)

UNCLASSIFIED

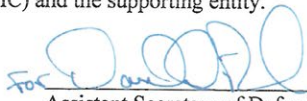
4. Conducting international cooperative RDT&E and information sharing with member nations of the North Atlantic Treaty Organization (NATO), with major non-NATO allies, or with any other ally or friendly foreign country, as authorized by 10 U.S.C. §§2350a-2350b;

5. Providing technology transition assistance associated with RDT&E efforts to DoD components and to non-DoD U.S. Government departments and agencies and foreign governments; facilitating the commercialization of capabilities developed through RDT&E efforts; and, as appropriate, facilitating the transition of capabilities to programs of record; and

6. Accepting and applying funds from DoD components, other U.S. Government departments and agencies, and foreign cooperative RDT&E partners to perform the foregoing functions in cooperation with or on behalf of the DoD component or interagency or foreign partner.⁸

Program Oversight and Support. The ASD (SO/LIC) exercises authority, direction, and control of the IWTSD, including budget authority, policy guidance, and oversight of any functions or missions described above. The provision of program support to the IWTSD, including contracting, finance, and security functions, will be by a designated DoD support office, as prescribed in a Memorandum of Understanding between the ASD (SO/LIC) and the supporting entity.

Dated: 04 JAN 2021



Assistant Secretary of Defense for Special Operations
and Low-Intensity Conflict

with applicable laws, regulations, and directives including the DoD Financial Management Regulation).

⁸ For purposes of this function, "funds" may include any applicable appropriation or foreign government contribution pursuant to a cooperative agreement or arrangement.

UNCLASSIFIED

(U) Army Contracting Command



DEPARTMENT OF THE ARMY
U.S. ARMY CONTRACTING COMMAND
4505 MARTIN ROAD
REDSTONE ARSENAL, AL 35898-5000

AMCC-IG

18 NOV 2022

MEMORANDUM THRU Headquarters, U.S. Army Materiel Command, Executive
Deputy To The Commanding General, 4400 Martin Road, Redstone Arsenal, AL
35898-5000

FOR Department of Defense, Inspector General, 4800 Mark Center Drive, Alexandria,
VA 22350-1500

SUBJECT: Army Contracting Command – Aberdeen Proving Ground (ACC-APG)
Responses to the Draft Report – Evaluation of Cybersecurity Controls on the DoD's
Secure Unclassified Network (Project No. D2022-DEV0PD-0082.000)

1. Reference: DoD Inspector General Draft Report–Evaluation of
Cybersecurity Controls on the DoD's Secure Unclassified Network (Project No.
D2022-DEV0PD-0082.000)
2. Upon review, I concur with the ACC-APG's responses and recommendations to the
draft report as set forth by DoD Inspector General. The enclosed responses are
sufficient and address the intent of the draft report.
3. I recommend DoD Inspector General accept the recommendations proposed by
ACC-APG and incorporate them into the final report – Evaluation of Cybersecurity
Controls on the DoD's Secure Unclassified Network.
4. The Army Contracting Command point of contact for this memorandum is [REDACTED]

2 Encls

1. Memorandum, ACC-RI, 17 Aug 21
2. DoD IG Draft Report, 4 Aug 21

CHRISTINE A. BEELER
Brigadier General, USA
Commanding

(U) Army Contracting Command (cont'd)



DEPARTMENT OF THE ARMY
U.S. ARMY CONTRACTING COMMAND - ABERDEEN PROVING GROUND
6472 INTEGRITY COURT, BUILDING 4401
ABERDEEN PROVING GROUND, MD 21005-3013

CCAP-OPC

16 November 2022

MEMORANDUM THRU LTC Jones, Inspector General, HQ U. S. Army Contracting Command, 4505 Martin Road, Redstone Arsenal, AL 35898-5000

FOR Mr. Bryan T. Clark, Program Director for Evaluations Overseas Contingency Operations, Department of Defense Inspector General, 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Response to Draft Report "Evaluation of Cybersecurity Controls on the DoD's Secure Unclassified Network," Project No. D022-DEV0PD-0082.000

1. Reference AMCC-IG (MAJ Jones) email, (Draft Report for the Evaluation of Cybersecurity Controls on the DoD's Secure Unclassified Network (Project No. D022-DEV0PD-0082.000)) 4 September 2022.
2. U.S. Army Contracting Command – Aberdeen Proving Ground comment on recommendation for subject evaluation are enclosed.
3. The point of contact is [REDACTED]

Encl

MITCHEM.MARTHAL Digitally signed by
 MITCHEM.MARTHAL
 Date: 2022.11.16 13:43:27 -05'00'

MARTHA L. MITCHEM
 Acting Executive Director

(U) Army Contracting Command (cont'd)

U.S. ARMY CONTRACTING COMMAND-ABERDEEN PROVING GROUND RESPONSE TO DRAFT REPORT "EVALUATION OF CYBERSECURITY CONTROLS ON THE DOD'S SECURE UNCLASSIFIED NETWORK," PROJECT No. D022-DEV0PD-0082.000

Background

The objective of this evaluation was to determine whether the DoD developed, implemented, maintained, and updated security and governance controls to protect the Secure Unclassified Network (SUNet), and the data and technologies that reside on it, from internal and external threats. SUNet allows the DoD, other U.S. Government agencies, and their partners, including academia, research, and foreign partners, to communicate, share, analyze, and disseminate information in near-real-time. SUNet supports more than a dozen agencies that have a range of missions, including building partner capacity, sharing information, and developing and testing artificial intelligence and machine learning. SUNet sponsors include the U.S. European Command, the U.S. Central Command, the Joint Interagency Task Force South, the Defense Intelligence Agency, the Joint Artificial Intelligence Center, and Project Maven.

U.S. Army Contracting Command – Aberdeen Proving Ground (ACC-APG) Adelphi Contracting Division issued and administers the SUNet contract on behalf of our mission partner, the Army Research Laboratory (ARL), in support of the Irregular Warfare Technical Support Directorate (IWTSD).

Overall, the draft audit report makes three recommendations with one specifically for ACC-APG.

Report Recommendation 1 for Executive Director, ACC-APG

We recommend that the Executive Director of the ACC-APG, Adelphi Contracting Division, in conjunction with the requiring activities:

- a. Conduct a review of the enterprise requirements and the performance work statement to determine whether the scope of the current contract should be revised to clearly support the Secure Unclassified Network's cybersecurity requirements and authority to operate.
- b. Conduct a review to determine how to increase transparency and communication between the Government parties to the contract to clarify how enterprise funding needs are determined and applied to Secure Unclassified Network enterprise requirements. And to ensure SUNet enterprise requirements are being fully executed as required.
- c. Conduct a review to determine whether a representative from the Irregular Warfare Technical Support Directorate, or any future designated Secure Unclassified Network mission owner or program office, should be the assistant or alternate contracting officer's representative on the SUNet infrastructure contract.

Enclosure

(U) Army Contracting Command (cont'd)

U.S. ARMY CONTRACTING COMMAND-ABERDEEN PROVING GROUND RESPONSE TO DRAFT REPORT "EVALUATION OF CYBERSECURITY CONTROLS ON THE DOD'S SECURE UNCLASSIFIED NETWORK," PROJECT No. D022-DEV0PD-0082.000

Response to Recommendation 1:

a. ACC-APG partially concurs with this recommendation. Our position is that this recommendation should be directed to the Army Research Laboratory (ARL) and the Irregular Warfare Technical Support Directorate (IWTSD). The Contracting Activity, in its role as business advisor is available to support the Requirement Activity (RA) and/or Program Manager (PM) in their review of the enterprise requirements and scope determinations and, upon that review with Mission Partner concurrence, the Contracting Activity will issue the appropriate contractual actions. However, this is an inherent function of the RA and/or PM. The Contracting Activity serves as a business advisor to the RA and/or PM to procure the necessary goods and services while ensuring compliance with Federal regulations and policies, reference Federal Contracting Regulation 1.602 Responsibilities. In our role as business advisors, ACC-APG will support discussions, with the RA and/or PM taking the lead, to determine whether the scope of the current contract should be revised to support the Secure Unclassified Network's cybersecurity requirements and authority to operate.

b. ACC-APG partially concurs with this recommendation. Our position is that this recommendation should be directed to the ARL and IWTSD. The Contracting Activity, in its role as business advisor is available to support the RA and/or PM in the increase of transparency and communications between multiple Government parties or obtain funding for the RA and/or PM's requirements. It is the RA and/or PM's responsibility to ensure adequate funding is provided to the Contracting Activity for obligation to the contract to allow for successful contract performance. In our role as business advisors, ACC-APG will support discussions, with the RA and/or PM taking the lead, to determine how to increase transparency and communication between Government parties and to clarify how enterprise funding needs are determined and applied to Secure Unclassified Network enterprise requirements.

c. ACC-APG concurs with this recommendation. ACC-APG Adelphi Contracting Division, in conjunction with the ARL, will determine whether a representative from the IWTSD, or any future designated Secure Unclassified Network mission owner or program office, should be the assistant or alternate contracting officer's representative on the SUNet infrastructure contract by 18 January 2023.

Enclosure

(U) Army Research Laboratory



DEPARTMENT OF THE ARMY
U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND
ARMY RESEARCH LABORATORY
OFFICE OF THE DIRECTOR
2800 POWDER MILL ROAD
ADELPHI, MARYLAND 20783-1138

FCDD-RL

MEMORANDUM FOR Program Director, Evaluations Overseas Contingency Operations, Office of Inspector General Department of Defense, 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: U.S. Army Combat Capabilities Development Command Army Research Laboratory Response to Draft Report for Project No. D2022-DEV0PD-0082.000

1. (U) The U.S. Army Combat Capabilities Development Command (DEVCOM) Army Research Laboratory (ARL) makes the following comments on the subject report in Enclosure 1:

a. (U) In the executive summary, the Office of Inspector General (OIG) report notes that Irregular Warfare Technical Support Directorate (IWTSD) "was unable to directly monitor and manage the execution of cybersecurity and information activities". The executive summary also says the IWTSD "was not able to ensure the implementation of cybersecurity activities because the direct monitoring of contractor performance was the responsibility of the Contracting Officer's Representative, which was staffed by the DEVCOM ARL." Pages 10 and 11 of the report paraphrase these statements.

(1) (U) The ARL disagrees with these statements. Page 3 of Enclosure 2, the IWTSD Technical Monitor (TM) Appointment Letter, shows the IWTSD TM is directly empowered by the Contracting Officer to "Monitor the contractor's performance; notify the contractor of deficiencies observed during surveillance and direct appropriate action to effect correction". The IWTSD TM is both authorized and required to directly monitor and manage execution of cybersecurity and information activities during performance of their duties.

(2) (U) Enclosure 3, the contractor's Secure Unclassified Network Monthly Status Report for September 2022, shows that the IWTSD TM provides daily monitoring and tasking of the contractor. Accomplishments 2, 4-8, 10 and 12 starting on page 3 all describe the contractor responding to IWTSD oversight, approval, and direction. Accomplishments 5, 8, 11 and 12 highlight how the IWTSD Change Control Board (CCB) reviews and approves all system changes. Pages 8 and 9 of Enclosure 3 show that the contractor had 34 meetings with IWTSD in September to support the CCB, program management, and Authority to Operate processes. As evidenced in this report, IWTSD monitors contract performance, notifies the contractor of performance deficiencies, and directs corrective actions.

CUI

Controlled By: U.S. Army Combat Capabilities Development Command Army Research Laboratory (DEVCOM-ARL)
Controlled By: FCDD-RL
CUI Category(ies): OPSEC INTL
Limited Dissemination Control: NOFORN
POC: [REDACTED]

(U) Army Research Laboratory (cont'd)

CUI

FCDD-RL

SUBJECT: U.S. Army Combat Capabilities Development Command Army Research Laboratory Response to Draft Report for Project No. D2022-DEV0PD-0082.000

(3) (U) The oversight activities under "The IWTSD Reviewed and Assessed SUNet Cybersecurity Controls" section on pages 10 and 11 of the OIG report in Enclosure 1 provides further examples of IWTSD's oversight and approval of all system architecture and maintenance through their ATO process.

b. (U) In the executive summary, the OIG report in Enclosure 1 states "SUNet did not have dedicated programmatic funding to support enterprise requirements and there was no designated entity obligated to fund enterprise requirements."

(U) The ARL disagrees with this statement. Per the "Fiscal Year 2022 Plans" on page 2 of the SUNet Appropriation at Enclosure 4, IWTSD was funded and directed by Congress to "manage and maintain a SUNet enterprise system" in FY22.

c. (U) The ARL concurs with Recommendation 1. The ARL will complete a review of requirements, work statement, communications and oversight of the SUNet Enterprise contract by 16 January 2023.

[REDACTED]

e. (U) The ARL concurs with Recommendation 3 but has a limited role in its execution.

2. (U) The ARL point of contact for this issue is [REDACTED]

[REDACTED]

4 Encls

BAKER.PATRIC^K
K.J. [REDACTED]
Digitally signed by
BAKER.PATRICK,
Date: 2022.11.16 17:23:25 -05'00'

PATRICK J. BAKER
Director

2

CUI

(U) Army Research Laboratory (cont'd)**TECHNICAL MONITOR NOMINATION AND APPOINTMENT****TECHNICAL MONITOR INFORMATION**

AKO Name: [REDACTED]

E-mail address: [REDACTED]

Office Symbol: CTTSO

Requiring Activity: CTTSO

Work Address: 4800 Mark Center Drive, Suite 13E13, Alexandria, VA 22350

Phone: [REDACTED]

DSN: _____

Job Title: Deputy Program Manager

Predominant Career Field 0340

Level of Certification: _____

Training Completed (Attach copies of certificates):

COURSE	COMPLETION DATE
CLC 222	10/8/19
CLM 003 or other Ethics	10/8/19
Combatting Trafficking in Persons	10/8/19
CLC 106	n/a

Supervisor Name: [REDACTED]

Supervisor Phone: [REDACTED]

Supervisor Email Address: [REDACTED]

CONTRACT INFORMATION

Contract Number: W911QX-19-C-0039

Delivery/Task Order Number: N/A

Contract Title: SUNet Infrastructure

Contracting Officer (KO): [REDACTED]

KO Phone: [REDACTED]

KO Email Address: [REDACTED]

Template last updated 8/3/2017

(U) Army Research Laboratory (cont'd)

COR: [REDACTED]

COR Phone: [REDACTED]

COR Email Address: [REDACTED]

CONCURRENCE FOR NOMINATION

TM Supervisor:

I hereby approve the above named individual to act as Technical Monitor on the named contract or order. His/her training and experience have prepared him/her to perform the duties associated with this position as outlined in the Quality Assurance Surveillance Plan. His/her work schedule allows adequate time to complete the tasking associated with performing as Technical Monitor.

X	RAMOS.GABRIE L.A. [REDACTED]	Digitally signed by RAMOS.GABRIE L.A. [REDACTED] Date: 2019.12.02 10:51:07 -0500
	Technical Monitor's Supervisor (Super)	

COR:

As COR for the above named contract or order, I hereby nominate the above named individual to serve as Technical Monitor in accordance with the duties outlined in the Quality Assurance Surveillance Plan. The nominated Technical Monitor meets the training requirements to serve in this position. My monthly reports will contain information obtained from the Technical Monitor regarding contractor performance.

X	TOTH.SUSAN.MAR GARET [REDACTED]	Digitally signed by TOTH.SUSAN.MARGARET [REDACTED] Date: 2019.12.02 11:58:15 -0500
	Contracting Officer's Representative (COR)	

APPOINTMENT

1. You are authorized by this designation to take action with respect to the following:

FORM CCAP-OP-02

(U) Army Research Laboratory (cont'd)

- a. Verify that the contractor performs the technical requirements of the contract in accordance with the contract terms, conditions and specifications. Specific emphasis should be placed on the quality provisions, for both adherence to the contract provisions and to the contractor's own quality control program.
 - b. Perform, or cause to be performed, inspections necessary in connection with paragraph 1a and verify that the contractor has corrected all deficiencies.
 - c. Maintain liaison and direct communications with the contractor. Written communications with the contractor and other documents pertaining to the contract shall be signed as "Technical Monitor" and a copy shall be furnished to the Contracting Officer's Representative (COR) and the contracting officer.
 - d. Monitor the contractor's performance; notify the contractor of deficiencies observed during surveillance and direct appropriate action to effect correction. Record and report to the contracting officer incidents of faulty or nonconforming work, delays or problems to the COR and the contracting officer. In addition, you are required to submit a monthly report concerning performance of services rendered under this contract to the COR.
 - e. Coordinate site entry for contractor personnel to include all necessary computer and network access, personnel badges for base and building access as well as all parking permits and decals. In addition, you are responsible for the turn in of any badges, permits, or decals upon the departure of these individuals. The site entry procedures taken shall be in accordance with the local base rules, regulations and policies.
 - f. Insure that any Government Furnished Property (GFP) is available when required.
2. You are not empowered to award, agree to or sign any contract (including delivery orders) or contract modification or in any way to obligate the payment of money by the Government. You may not take any action that may affect contract or delivery order schedules, funds or scope. All contractual agreements, commitments or modifications that involve price, quantity, quality, delivery schedules or other terms and conditions of the contract must be made by the contracting officer. You may be personally liable for unauthorized acts. You may not re-delegate your TM authority.
 3. This designation as a TM shall remain in effect through the life of the

FORM CCAP-OP-02

(U) Army Research Laboratory (cont'd)

contract, unless sooner revoked in writing by the contracting officer or unless you are separated from Government service. If you are to be reassigned or to be separated from Government service, you must notify the contracting officer sufficiently in advance of reassignment or separation to permit timely selection and designation of a successor TM. If your designation is revoked for any reason before completion of this contract, turn your records over to the successor TM and COR or obtain disposition instructions from the contracting officer.

4. You are required to maintain adequate records to sufficiently describe the performance of your duties as a TM during the life of this contract and to dispose of such records as directed by the contracting officer. As a minimum, the TM file must contain the following:
 - a. A copy of your letter of appointment from the contracting officer, a copy of any changes to that letter and a copy of any termination letter. A copy of your formal training.
 - b. A copy of the contract or the appropriate part of the contract and all contract modifications. (TM must maintain a file of the contract and all modifications either electronically or paper copies)
 - c. A copy of the applicable quality assurance (QASP) surveillance plan.
 - d. All correspondence initiated by authorized representatives concerning performance of the contract.
 - e. A record of inspections performed and the results.
 - f. Memoranda for record or minutes of any pre-performance conferences.
 - g. Memoranda for record of minutes of any meetings and discussions with the contractor or others pertaining to the contract or contract performance.
 - h. Applicable laboratory test reports.
 - i. Records relating to the contractor's quality control system and plan and the results of the quality control effort.
 - j. A copy of the surveillance schedule.
 - k. Documentation pertaining to your inspection of performance of services, including reports and other data.

FORM CCAP-OP-02

(U) Army Research Laboratory (cont'd)

5. At the time of contract completion, you will ensure all records are provided to the COR.
6. All personnel engaged in contracting and related activities shall conduct business dealings with industry in a manner above reproach in every aspect and shall protect the U.S. Government's interests, as well as maintain its reputation for fair and equal dealings with all contractors. DoD Directive 5500.7-R sets forth standards of conduct for all personnel directly and indirectly involved in contracting.
7. A TM who may have direct or indirect financial interests which would place the TM in a position where there is a conflict between the TMs private interests and the public interests of the United States shall advise the supervisor and the contracting officer of the conflict so that appropriate actions may be taken. TMs shall avoid the appearance of a conflict of interests in order to maintain public confidence in the U.S. Government's conduct of business with the private sector. TMs must supply the Contracting Officer with evidence that she/he has officially filed an OGE Form 450 Confidential Financial Disclosure Report each February. This information shall be provided to the COR for the February Monthly COR Report.
8. You are required to acknowledge receipt of this TM designation and return it to the contracting officer electronically. Your signature also serves as certification that you have read and understand the contents of DoD Directive 5500.7-R. The original copy of this designation should be retained for your file.
9. William Nuamah, 301-394-0755, is your point of contact for this action.


10. Attachments I: Quality Assurance Surveillance Plan (QASP)

Technical Monitor:

I understand my duties listed above as well as outlined in the Quality Assurance Surveillance Plan. If during contract performance I can no longer serve as Technical Monitor, I will notify the COR and Contracting Officer to allow adequate time for a replacement Technical Monitor to be appointed.


FORM CCAP-OP-02

(U) Army Research Laboratory (cont'd)

 EASON, JULIA Digitally signed by EASON, JULIA Date: 2019.11.27 12:51:37 -05'00'
Technical Monitor (Tech)

Contracting Officer:

The above named individual is appointed to perform Technical Monitor duties as outlined in the Quality Assurance Surveillance Plan.

 MOLINA, SERGIO J AVIER Digitally signed by MOLINA, SERGIO JAVIER Date: 2019.12.03 11:50:34 -05'00'
Contracting Officer (KO)

FORM CCAP-OP-02

(U) Army Research Laboratory (cont'd)

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense										Date: April 2022		
Appropriation/Budget Activity					R-1 Program Element (Number/Name)							
0400: Research, Development, Test & Evaluation, Defense-Wide / BA 3: Advanced Technology Development (ATD)					PE 0603121D8Z / SO/LIC Advanced Development							
COST (\$ in Millions)	Prior Years	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total	FY 2024	FY 2025	FY 2026	FY 2027	Cost To Complete	Total Cost
Total Program Element	4.847	4.904	4.665	4.919	-	4.919	5.072	5.180	5.200	5.304	-	
121: SO/LIC Advanced Development	4.847	4.904	4.665	4.919	-	4.919	5.072	5.180	5.200	5.304	-	-
Quantity of RDT&E Articles	-	-	-	-	-	-	-	-	-	-		

Note
New Start (Y/N): No

A. Mission Description and Budget Item Justification
This program supports the Department's initiatives to Deter Aggression, Defend the Homeland, and Build Sustainable and Long-Term Advantage.

The SUNet enterprise system is an unclassified, secure information platform that allows the user to communicate, analyze, and share information between defense, interagency, and foreign partners. Rested on SUNet are mission specific enclaves used to detect, monitor, understand, and act in the information environment. The SUNet system provides defense and interagency partners with an accredited platform that enables secure unclassified information sharing, joint analysis, and advanced RDT&E in support of critical operational missions on a global scale. The platform currently supports more than a dozen sponsoring agencies with a range of missions, including but not limited to research and analysis of publicly available information, Phase 0 shaping, informing and influencing; building partner capacity; and enables rapid, iterative development and fielding of artificial intelligence and machine learning. The SUNet platform enables IWTSD to identify and develop capabilities to combat terrorism and irregular adversaries, and deliver these capabilities to DoD components and interagency partners with a provision of support to US military operations.

B. Program Change Summary (\$ in Millions)	FY 2021	FY 2022	FY 2023 Base	FY 2023 OCO	FY 2023 Total
Previous President's Budget	4.904	4.665	0.000	-	0.000
Current President's Budget	4.904	4.665	4.919	-	4.919
Total Adjustments	0.000	0.000	4.919	-	4.919
• Congressional General Reductions	-	-			
• Congressional Directed Reductions	-	-			
• Congressional Rescissions	-	-			
• Congressional Adds	-	-			
• Congressional Directed Transfers	-	-			
• Reprogrammings	-	-			
• SBIR/STTR Transfer	-	-			
• Adjustment to Budget Year	-	-	4.919	-	4.919

PE 0603121D8Z: SO/LIC Advanced Development
Office of the Secretary Of Defense

UNCLASSIFIED
Page 1 of 3

R-1 Line #30

Volume 3 - 109

(U) Army Research Laboratory (cont'd)

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022	
Appropriation/Budget Activity 0400: <i>Research, Development, Test & Evaluation, Defense-Wide / BA 3: Advanced Technology Development (ATD)</i>		R-1 Program Element (Number/Name) PE 0603121D8Z / <i>SO/LIC Advanced Development</i>	
Change Summary Explanation FY 2023 funding increase reflects the fact that the FY 2022 President's Budget request did not include out-year funding.			
C. Accomplishments/Planned Programs (\$ in Millions)		FY 2021	FY 2022
Title: Secure, Unclassified Network (SUNet)		4.904	4.665
Description: The SUNet enterprise system is an unclassified, secure information platform that allows the user to communicate, analyze, and share information between defense, interagency, and foreign partners. Rested on SUNet are mission specific enclaves used to detect, monitor, understand, and act in the information environment. The SUNet system provides defense and interagency partners with an accredited platform that enables secure unclassified information sharing, joint analysis, and advanced RDT&E in support of critical operational missions on a global scale. The platform currently supports more than a dozen sponsoring agencies with a range of missions, including but not limited to research and analysis of publicly available information, Phase 0 shaping, informing and influencing; building partner capacity; and enables rapid, iterative development and fielding of artificial intelligence and machine learning. The SUNet platform enables IWTSD to identify and develop capabilities to combat terrorism and irregular adversaries, and deliver these capabilities to DoD components and interagency partners with a provision of support to US military operations.			4.919
FY 2022 Plans: Expand the Competitive Space. Continue an effort to develop, integrate, test, deploy, manage and maintain a SUNet enterprise system with an emphasis on enhanced network engineering, information assurance, cybersecurity monitoring, enterprise governance, policy support, system redundancy and failover to efficiently and effectively support a growing number of users and missions across the platform.			
FY 2023 Plans: Expand the Competitive Space. Continue an effort to develop, integrate, test, deploy, manage and maintain a SUNet enterprise system with an emphasis on enhanced network engineering, information assurance, cybersecurity monitoring, enterprise governance, policy support, system redundancy and failover to efficiently and effectively support a growing number of users and missions across the platform.			
FY 2022 to FY 2023 Increase/Decrease Statement: There is no significant change between FY 2022 and FY 2023.			
Accomplishments/Planned Programs Subtotals		4.904	4.665
D. Other Program Funding Summary (\$ in Millions) N/A			
Remarks			

PE 0603121D8Z: *SO/LIC Advanced Development*
Office of the Secretary Of Defense

UNCLASSIFIED
Page 2 of 3

R-1 Line #30

Volume 3 - 110

(U) Army Research Laboratory (cont'd)

UNCLASSIFIED

Exhibit R-2, RDT&E Budget Item Justification: PB 2023 Office of the Secretary Of Defense		Date: April 2022
Appropriation/Budget Activity 0400: <i>Research, Development, Test & Evaluation, Defense-Wide / BA 3: Advanced Technology Development (ATD)</i>		R-1 Program Element (Number/Name) PE 0603121D8Z / <i>SO/LIC Advanced Development</i>
E. Acquisition Strategy N/A		

PE 0603121D8Z: *SO/LIC Advanced Development*
Office of the Secretary Of Defense

UNCLASSIFIED
Page 3 of 3

R-1 Line #30

Volume 3 - 111

(U) Acronyms and Abbreviations

(U) ARL	Army Research Laboratory
(U) ATO	Authority to Operate
(U) COR	Contracting Officer's Representative (lowercase in text)
(U) eMASS	Enterprise Mission Assurance Support Service
(U) IWTSD	Irregular Warfare Technical Support Directorate
(U) NIST	National Institute for Standards and Technology
(U) PWS	Performance Work Statement (lowercase in text)
(U) RMF	Risk Management Framework
(U) SUNet	Secure Unclassified Network
(U) TM	Technical Monitor (lowercase in text)

CUI



CUI

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

CUI



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

CUI