Report No. DODIG-2023-098

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

JULY 27, 2023

(U) Audit of the DoD's Accountability of Public Key Infrastructure Tokens Used to Access the Secret Internet Protocol Router Network

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: PROCURE~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC:~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Audit of the DoD's Accountability of Public Key Infrastructure Tokens Used to Access the Secret Internet Protocol Router Network

July 27, 2023

(U) Objective

(U) The objective of this audit was to determine whether the DoD managed and accounted for the Public Key Infrastructure (PKI) tokens used to access the Secret Internet Protocol Router Network (SIPRNet) in accordance with Federal and DoD Guidance. We performed this audit in response to a request from the Acting Director of Operational Test and Evaluation (DOT&E) and to address the allegation submitted to the DoD Hotline.

(U) Background

(U) The DoD PKI refers to the framework and services needed to issue, maintain, and revoke public key certificates. A public key certificate is a trusted digital identity used to identify users and devices when communicating over networks, and it is typically encoded on a token. In 1999, the National Security Agency was assigned Program Management Office (PMO) responsibilities for the DoD PKI Program. Since December 2012, the DoD has used SIPRNet tokens to access the SIPRNet. The DoD uses two SIPRNet tokens—SafeNet and Second Source Tokens—that support similar functionality but are produced by different manufacturers.

(U) The DoD PKI PMO manages SafeNet token orders while the Defense Manpower Data Center (DMDC) manages Second Source Token orders for DoD Components. DoD Components are responsible for managing SIPRNet tokens throughout their life cycle once they receive them.

(U) Finding

(U) Before April 2022, DoD PKI PMO and DMDC officials did not effectively manage orders, storage, or delivery of SIPRNet tokens, resulting in inaccurate token inventories. DoD PKI PMO and DMDC officials did not have accountability of SIPRNet tokens because inventory procedures were ineffective or nonexistent. However, in March and April 2022, the DoD PKI PMO implemented additional controls over the token ordering, storage, and delivery processes and a quarterly reconciliation process to improve accountability of SIPRNet tokens.

(U) In addition, the DMDC did not have financial records, such as invoices and Military Interdepartmental Purchase Requests, to support any SIPRNet token purchases made in 2017, and it could only partially support token purchases made during 2018 through 2020. However, the DMDC provided financial records supporting all token purchases made in 2021.

(U) The DMDC did not maintain complete financial records because the DMDC personnel responsible for SIPRNet token orders did not have a repository to transfer any information or upload documents. In November 2022, the DMDC updated its procedures to require DMDC personnel to store all financial records for SIPRNet token orders in a central repository. However, DMDC officials began working with DoD Components to collect and store financial documentation to support FY 2021 token purchases while updating the November 2022 procedures.

(U) Inaccurate token inventories resulted in the DoD Components purchasing tokens that they may not have needed. Implementing more stringent controls for managing SIPRNet tokens and maintaining accurate financial records, such as those implemented by the DoD PKI PMO and the DMDC during our audit, improve accountability, enable the DoD to trace tokens to specific purchases, reduce unnecessary expenditures for tokens that may not be needed, and improve financial reporting.

(U) Because the DoD PKI PMO and the DMDC took corrective actions during the audit, we did not make recommendations in this report.


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

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

July 27, 2023

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE MANPOWER DATA CENTER
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: (U) Audit of the DoD's Accountability of Public Key Infrastructure Tokens Used to Access the Secret Internet Protocol Router Network (Report No. DODIG-2023-098)

(U) This final report provides the results of the DoD Office of Inspector General's Audit of the DoD's Accountability of Public Key Infrastructure Tokens Used to Access the Secret Internet Protocol Router Network. We are providing this report for information and use. This report does not contain recommendations. We coordinated a discussion draft of this report with officials from the Director of Operational Test and Evaluation, the Defense Manpower Data Center, the Joint Interoperability Test Command, and DoD Public Key Infrastructure Program Management Office. They agreed with our report and provided technical comments, which we incorporated, as appropriate.

(U) If you have any questions or would like to meet to discuss the audit, please contact me [redacted] We appreciate the cooperation and assistance received during the audit.

FOR THE INSPECTOR GENERAL:

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether the DoD managed and accounted for Public Key Infrastructure (PKI) tokens used to access the Secret Internet Protocol Router Network (SIPRNet) in accordance with Federal and DoD guidance. We performed this audit in response to a request from the Acting Director of Operational Test and Evaluation (DOT&E) and to address the allegation submitted to the DoD Hotline. See Appendix A for the details on the audit scope and methodology.

(U) Background

(U) The DoD PKI refers to the framework and services needed to issue, maintain, and revoke public key certificates. A public key certificate is a trusted digital identity used to identify users and devices when communicating over networks and is typically encoded on a token.[1] DoD Instruction 8520.02 assigns the DoD PKI Program Management Office (PMO) with responsibility for managing the DoD's PKI.[2] In 1999, the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence assigned the National Security Agency with program management responsibilities for the DoD PKI Program.[3]

(U) The DoD uses PKI to limit access to DoD networks and data to only authorized individuals and devices across the DoD Information Network.[4] The DoD PKI also enables authorized individuals to encrypt and digitally sign e-mails, protecting the content of the e-mail messages and verifying the identity of the sender. SIPRNet tokens with loaded user certificates are the primary credential for managing logical authentication to the SIPRNet, which is the DoD's network for processing, storing, and transmitting classified information and messages containing up to

[1] (U) A token is a credit-card sized smartcard embedded with a microchip that stores, processes, and communicates information.

[2] (U) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011 (Updated May 18, 2023).

[3] (U) Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence Memorandum, "Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure," April 9, 1999. In January 2012, the DoD Chief Information Officer assumed the authorities and responsibilities of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.

[4] (U) The DoD Information Network is the DoD's globally interconnected, end-to-end set of electronic information capabilities and associated processes for collecting, processing, storing, disseminating, and managing digital information on-demand to warfighters, policy makers, and support personnel.

(U) collateral SECRET information. SIPRNet tokens without user credentials cannot be used to access the SIPRNet. The DoD has used SIPRNet tokens since December 2012 for controlling access to the SIPRNet. A SIPRNet token's life cycle includes activities to obtain, manage, distribute, issue, and destroy a token.

(U) The DoD PKI PMO manages SIPRNet tokens through the SIPRNet Token Management System (TMS). The TMS provides certificate registration, issuance, validation, revocation, personal identification number reset, token rekey, suspension and restoration, and maintenance support for SIPRNet users. The Central Management of Tokens database is a portal within the TMS that is used by the DoD PKI PMO, Military Services, and Defense agencies to:

- (U) transfer tokens between DoD Components,
- (U) provide privileges and access within Central Management of Tokens to Token Inventory Managers,
- (U) view token inventory,
- (U) perform inventory-related searches, and
- (U) generate inventory-related reports.

(U) Acting Director Concerns on SIPRNet Tokens Management and Accountability

(U) In a September 14, 2021, memorandum to the DoD Inspector General and the National Security Agency Director, the Acting DOT&E identified concerns regarding approximately 143,000 SIPRNet tokens valued at $1.4 million. The Joint Interoperability Test Command found that the DoD PKI PMO and Defense Manpower Data Center (DMDC) could not establish accountability for the approximately 143,000 SIPRNet tokens during operational testing.[5] The Acting Director specifically cited issues with the token ordering process and the lack of a token reconciliation process.

(U) The Joint Interoperability Test Command found that the DoD PKI PMO and Defense Manpower Data Center (DMDC) could not establish accountability for the approximately 143,000 SIPRNet tokens during operational testing.

[5] (U) Director, Operational Test and Evaluation, "Updated Public Key Infrastructure (PKI) Increment 2 Follow-On Operational Test And Evaluation (FOT&E) Report," November 2021. The Joint Interoperability Test Command conducted the Follow-On Operational Test and Evaluation for the DOT&E. For the purpose of our report, "accountability" refers to the ability to identify which DoD Components owned the tokens in the manufacturer's vault.

(U) The Acting Director requested that the DoD Office of Inspector General conduct an independent reconciliation of SIPRNet tokens. To conduct the independent reconciliation, we reviewed SIPRNet token orders from October 2017 through September 2021 in the TMS and validated the accuracy of the TMS data using invoices, Military Interdepartmental Purchase Requests (MIPRs), and delivery orders.

(U) DoD Hotline Allegation

(U) On October 5, 2021, the DoD Hotline received an allegation concerning SIPRNet token accountability. The complainant alleged that the DoD PKI PMO did not have full accountability of SIPRNet tokens.

(U) Token User Responsibilities

(U) To assess the overall accountability of tokens that had been issued to token users, we conducted limited testing to determine whether we should expand the scope of this review to also look at the accountability of tokens when in the possession of users. We did not identify any issues with accountability of issued tokens and, as a result, focused our audit on the token ordering and distribution process at the DoD PKI PMO level. See Appendix B for the results of our review of whether 107 nonstatistically selected users from six DoD Components were in possession of assigned SIPRNet tokens.

(U) DoD PKI PMO and Defense Manpower Data Center Responsibilities for SIPRNet Token Ordering Process

(U) The DoD uses two SIPRNet tokens—SafeNet and Second Source Tokens (SSTs)—that support similar functionality but are produced by different manufacturers. The DoD PKI PMO manages SafeNet token orders while the DMDC manages SST orders. Neither SafeNet nor SSTs contain user credentials and therefore do not represent a security risk until the DoD Components issue them to users.

~~(CUI)~~ The DoD PKI PMO established standard operating procedures (SOPs) and [redacted]

(U) In March and April 2022, the DoD PKI PMO updated the procedures for ordering SST and SafeNet tokens, and it created a process to reconcile SIPRNet token orders.[7] The updated procedures required additional oversight and controls, such as:

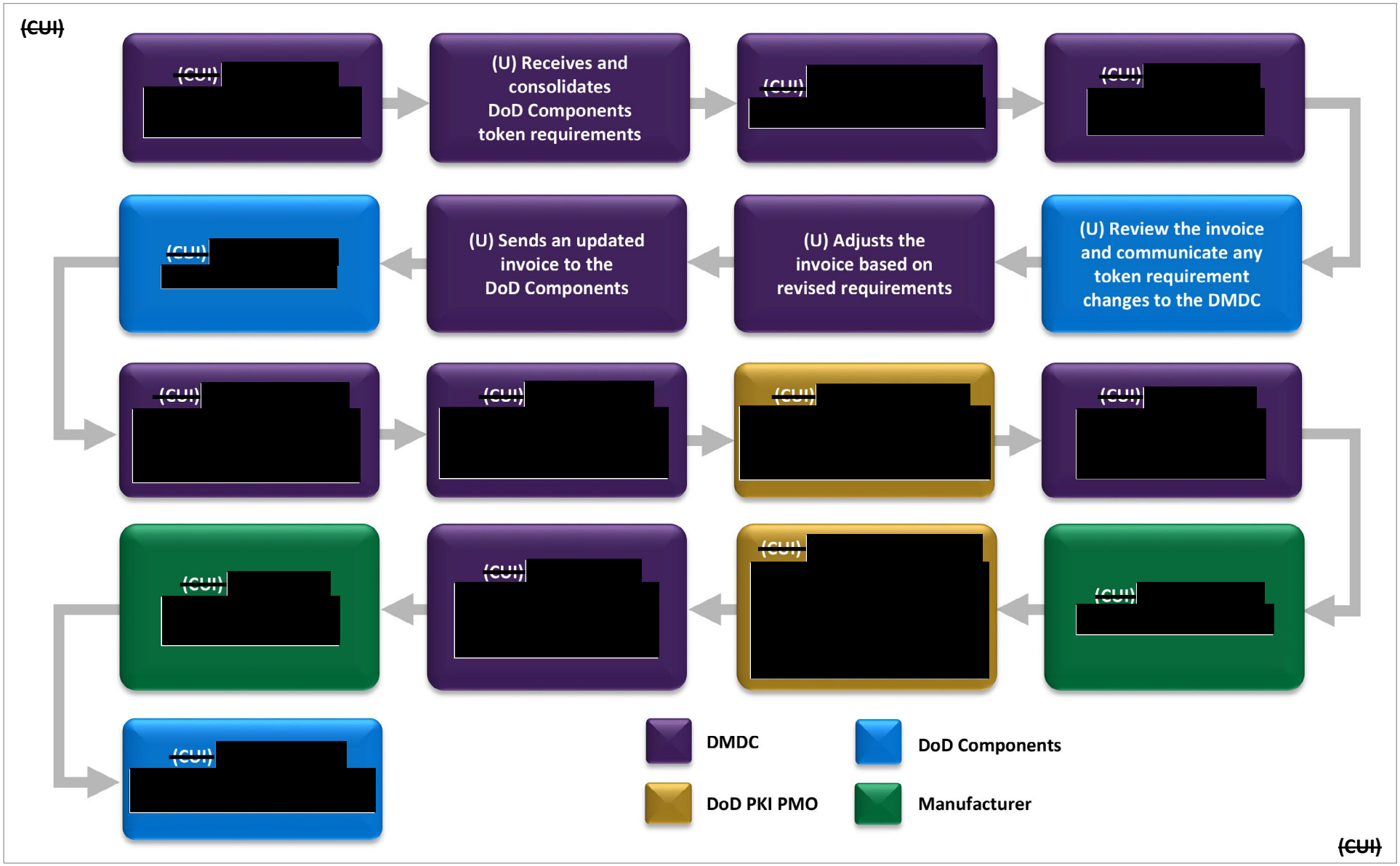
- (U) shipping tokens directly to DoD Components instead of storing the tokens in the manufacturer's vault;
- (U) reconciling SIPRNet token orders each quarter; and
- ~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted] The following figure details the updated SST ordering process.

[6] (U) DoD PKI PMO, "Standard Operating Procedure (SOP) for Services and Agencies (S/As) Inventory Management," Version 1.0, May 15, 2017.
(U) "SIPRNET Token Management System (TMS) Central Management of Tokens (CMT) Portal User Guide," February 28, 2020.

[7] (U) DoD PKI PMO, "SIPRNET Token Ordering Reconciliation Standard Operating Procedure," Version 1.0, March 2022.
(U) DoD PKI PMO, "Enterprise Token Ordering and Fulfillment Standard Operating Procedure," Version 2.1, April 2022.

~~(CUI)~~ Figure. Updated SST Ordering Process and Associated Responsibilities



(U) Source: The DoD OIG.

~~(CUI)~~ [redacted]

The DoD PKI PMO processes the DoD Components' SafeNet token orders with the manufacturer, which is responsible for shipping the tokens directly to the Components once manufacturing is complete.

(U) DoD Component Responsibilities for Managing SIPRNet Tokens after Receipt of Tokens

~~(CUI)~~ DoD Components are responsible for managing SIPRNet tokens throughout the tokens' life cycle once they receive the tokens. [redacted]

~~(CUI)~~ According to the National Security Systems PKI DoD Registration Practice Statement, DoD Component Registration Authority (RA) Officers are responsible for maintaining token inventories within their respective Components.[9] RA Officers should only issue SIPRNet tokens after verifying a user's identity [redacted] RA Officers are also responsible for destroying tokens not intended for reuse using approved methods, such as a shredder approved for destroying classified material.

(U) Review of Internal Controls

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[10] We identified internal control weakness at the DoD PKI PMO concerning the accountability of SIPRNet tokens and at the DMDC concerning its ability to support SIPRNet token orders and the cost of those orders. We will provide a copy of the report to the senior official responsible for internal controls in the DoD PKI PMO and the DMDC.

[8] (U) DoD PKI PMO, "Standard Operating Procedure (SOP) for Services and Agencies (S/As) Site Management," Version 1.0, April 2022.
(U) "SIPRNET Token Management System (TMS) Central Management of Tokens (CMT) Portal User Guide," February 28, 2020.

[9] (U) National Security System PKI DoD Registration Practice Statement, Version 14, July 13, 2022. An RA is an entity authorized by the DoD components to collect, verify, and submit information provided by potential users for the purpose of issuing public key certificates.

[10] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013 (Incorporating Change 1, June 30, 2020).

(U) Finding

(U) The DoD PKI PMO and the DMDC Implemented Controls to Improve Accountability of and Support for SIPRNet Token Purchases

(U) Before April 2022, DoD PKI PMO and DMDC officials did not effectively manage orders, storage, or delivery of SIPRNet tokens, resulting in inaccurate token inventories. DoD PKI PMO and DMDC officials did not have accountability of SIPRNet tokens because procedures were ineffective or nonexistent. However, in March and April 2022, the DoD PKI PMO implemented additional controls over the token ordering, storage, and delivery processes, and a quarterly reconciliation process to improve accountability of SIPRNet tokens.

(U) In addition, the DMDC did not have financial records, such as invoices and MIPRs, to support any SIPRNet token purchases made in 2017, and it could only partially support token purchases made during 2018 through 2020. However, the DMDC provided financial records supporting all token purchases made in 2021. The DMDC did not maintain complete financial records because the DMDC personnel responsible for SIPRNet token orders did not have a repository to transfer information or upload documents. In November 2022, the DMDC updated its procedures to require DMDC personnel to store all financial records for SIPRNet token orders in a central repository.

(U) Inaccurate token inventories can and has resulted in the DoD Components purchasing tokens that they may not have needed. For example, the Army and the Defense Health Agency purchased additional SIPRNet tokens without depleting SIPRNet tokens in the manufacturer's vault that they already purchased. Implementing more stringent controls for managing SIPRNet tokens and maintaining accurate financial records, such as those implemented by the DoD PKI PMO and the DMDC during our audit, improve accountability, enable the DoD to trace tokens to specific purchases, reduce unnecessary expenditures for tokens that may not be needed, and improve financial reporting.

(U) The DoD PKI PMO Took Action to Improve Accountability of SIPRNet Tokens

(U) Before April 2022, DoD PKI PMO and DMDC officials did not effectively manage orders, storage, or delivery of SIPRNet tokens, resulting in inaccurate token inventories. However, the DoD PKI PMO took actions to address SIPRNet token management and accountability issues, including those identified by the DOT&E office during a November 2021 Follow-On Test and Evaluation, by:

- (U) updating procedures;
- (U) requiring additional controls over the token ordering, storage, and delivery processes; and
- (U) implementing a quarterly reconciliation process to ensure the accuracy of the token management process.

(U) Updated SIPRNet Token Ordering Process

(U) The DoD PKI PMO updated its SOP in April 2022 for the SIPRNet token ordering process that required additional controls to verify token quantities and shipping instructions for each order, which addressed the issues identified by the DOT&E in its November 2021 operational test report. In the November 2021 report, the DOT&E reported that the DoD PKI PMO shipped 45,000 SSTs to the Air Force that the Air Force did not purchase. Before the updated processes were implemented, the DMDC told the DoD PKI PMO how many tokens were ordered without verifying the accuracy of the order, and the DoD PKI PMO entered that quantity in the TMS.

~~(CUI)~~ The updated SOP requires the use of a data package, which includes a Card Buy Record, MIPRs, MIPR acceptances, and invoices. [redacted] The Card Buy Record lists the SST quantities ordered by each DoD Component. For example, DoD PKI PMO official provided a spreadsheet for the 2022 SIPRNet token order that they used to track DoD Component concurrence on the data package token quantities before entering the data in the TMS.

(U) The additional requirements and implemented steps to validate SIPRNet token orders addressed the issues with the accuracy of token orders. Therefore, we did not recommend further corrective actions in this report.

(U) Updated SIPRNet Token Storage and Delivery Processes

~~(CUI)~~ [redacted] In its November 2021 report, the DOT&E reported that the Joint Interoperability Test Command identified approximately 143,000 unaccounted SIPRNet tokens in the manufacturer's vault. The DOT&E later explained that the Joint Interoperability Test Command determined that the DoD PKI PMO and DMDC could not identify which DoD Components owned the approximately 143,000 SIPRNet tokens in the manufacturer's vault. Before implementing the updated process, DoD Components did not always receive all SIPRNet tokens ordered at one time. Instead, DoD Components requested SIPRNet tokens from the manufacturer as they needed them.

(U) The remaining SIPRNet tokens from specific orders were stored in the manufacturer's vault. For example, the Army ordered 90,000 SSTs but only requested two shipments of 20,000 tokens each, leaving 50,000 Army-purchased SSTs in the vault. In addition, the Defense Health Agency ordered 450 SSTs, but it never requested tokens; therefore, the tokens remained in the manufacturer's vault. In subsequent years, the Army and the Defense Health Agency purchased additional SIPRNet tokens without depleting all of the tokens stored in the manufacturer's vault.

~~(CUI)~~ [redacted] According to the updated SOP, the DoD PKI PMO is required to contact DoD Component PKI personnel to verify token orders were delivered if TMS was not updated within the 2-week period.

(U) The changes implemented by the DoD PKI PMO to the ordering and delivery processes eliminated the practice of storing tokens in the manufacturer's vault and increased accountability of SIPRNet token orders. Therefore, we did not recommend further corrective actions in this report.

(U) Implemented SIPRNet Token Order Reconciliation Process

(U) The DoD PKI PMO developed and implemented an SOP in March 2022 for reconciling SIPRNet token orders. The SOP requires the DoD PKI PMO to conduct quarterly reconciliations by comparing token order quantities identified on supporting documentation, such as invoices and MIPRs, to the token quantities included on the Card Buy Records. The SOP also requires the DMDC to review and sign the completed reconciliation reports, indicating agreement with the reconciliation conducted by the DoD PKI PMO.

(U) In its November 2021 report, the DOT&E reported that the DoD did not conduct or document an independent reconciliation of any SIPRNet token orders. Specifically, the DOT&E reported that the Joint Interoperability Test Command identified approximately 143,000 SIPRNet tokens that were unaccounted for in the manufacturer's vault. The DOT&E later explained that the Joint Interoperability Test Command determined that the DoD PKI PMO and DMDC could not identify which DoD Components owned the approximately 143,000 SIPRNet tokens in the manufacturer's vault. In addition, DOT&E officials stated that the approximately 143,000 unaccounted for SIPRNet tokens was an estimate based on partial records and interviews with the DoD PKI PMO and the DMDC during operational testing from November 2020 through March 2021.

(U) In response to the DOT&E's findings, the DoD PKI PMO took steps to reconcile the tokens and identified that the vault contained approximately 132,000 SIPRNet tokens. In September 2021, the DoD PKI PMO directed the manufacturer to begin shipping the tokens in the manufacturer's vault to the DoD Components that had previously purchased them, and the shipments were completed in February 2023.

(U) The DoD PKI PMO completed its first reconciliation to verify the accuracy of token order purchases based on SOP requirements in April 2022, and has since completed seven others. During the May 2022 reconciliation, the DoD PKI PMO identified and quickly corrected a misshipped order. Specifically, the DoD PKI PMO identified that it directed the manufacturer to ship an order for 100 tokens for the National Geospatial-Intelligence Agency to the Missile Defense Agency in error. The May 2022 reconciliation process resulted in the DoD PKI PMO correcting the error in a timely manner by having the Missile Defense Agency ship the tokens directly to the National Geospatial-Intelligence Agency.

(U) Since implementing the SOP, the PMO has conducted eight reconciliations. We reviewed the May 2022 reconciliation for the September 2021 SST order and determined that the DoD PKI PMO followed its procedures by verifying documentation that supported the cost and quantity for the September 2021 SST order. The actions taken by the DoD PKI PMO to implement a quarterly reconciliation process to verify SIPRNet token orders and address errors in the ordering, delivery, and receipt processes improved accountability. Therefore, we did not recommend further corrective actions in this report.

(U) The actions taken by the DoD PKI PMO to implement a quarterly reconciliation process to verify SIPRNet token orders and address errors in the ordering, delivery, and receipt processes improved accountability.

(U) The DMDC Did Not Maintain Records to Support SIPRNet Token Orders

(U) The DMDC provided financial records, such as invoices and MIPRs, supporting SIPRNet token purchases made in 2021 but did not have financial records to support any token purchases made in 2017 and provided financial records that partially supported token purchases made during 2018 through 2020. The DoD Financial Management Regulation requires the DoD to maintain financial transaction records for goods and services for a minimum of 10 years.[11] Table 1 summarizes SIPRNet token purchases by year, the quantity ordered with TMS through the Card Buy Record, the quantity shown on invoices, and the inconsistencies between the quantity within TMS and the invoices.

(U) Table 1. Summary of SIPRNet Token Purchases from 2017 Through 2021 and Inconsistencies Between the Card Buy Record and Invoices

(U) Year	DoD Components with SIPRNet Token Orders	Card Buy Record SIPRNet Token Only	Invoice SIPRNet Token Quantity	Inconsistency for SIPRNet Token Quantities
2017	15	362,800	0	362,800
2018	10	152,700	84,250	68,450
2019	14	325,200	170,450	154,750
2020	15	127,900	125,800	2,100
2021	16	173,000	173,000	0
Total	**70**	**1,141,600**	**553,500**	**588,100** (U)

(U) Source: The DoD OIG.

(U) To determine whether SIPRNet token purchases were supported by financial records, we obtained invoices, MIPRS, and Card Buy Records. Based on the information obtained, we identified inconsistencies including:

- (U) in 2018, the Card Buy Record showed the Army ordered 117,450 tokens, but the invoice supported only 50,000 SIPRNet tokens;
- (U) in 2019, the Card Buy Record showed the Marine Corps ordered 15,500 tokens, but the invoice supported only 15,200 SIPRNet tokens;

[11] (U) DoD Regulation 7000-14R, "DoD Financial Management Regulation," Volume 1, Chapter 9.

- (U) in 2020, the Card Buy Record showed the Joint Service Provider ordered 15,200 tokens, but the invoice supported only 15,000 SIPRNet tokens; and
- (U) from October 2017 through September 2021, the Card Buy Records showed the Defense Health Agency ordered 2,950 tokens, but the invoices supported only 1,200 SIPRNet tokens.

(U) The DMDC used a records management file plan to determine how long to maintain documents, including the retention requirements for financial records related to procuring goods. The DMDC Customer Relationship Management Director stated that although the DMDC records retention policy required the DMDC to keep financial records for 7 years, the DMDC did not maintain complete financial records because the DMDC personnel responsible for SIPRNet token orders did not have a repository to transfer any information or upload documents.

(U) In November 2022, the DMDC revised its Token Management SOP to require DMDC personnel to file cost estimates, funding documents, and solicitation e-mails and responses on a shared drive in separate folders by fiscal year.[12] While the DMDC completed its revised Token Management SOP, DMDC officials worked with DoD Components to collect and store financial documentation to support FY 2021 token purchases based on preliminary issues identified during Joint Interoperability Test Command operational testing. We verified that the DMDC electronically stored the required information for SIPRNet token purchases made since the start of FY 2022 in accordance with its updated procedures. We also verified the type of documents being stored in the repository, such as initial cost estimates and customer e-mails, are in accordance with the updated procedures.

(U) In addition, the DMDC began following the Office of the Secretary of Defense Records and Information Management Program records retention and records disposition schedules requirements updates in January 2023, which aligns with the DoD Financial Management Regulations for financial transactions requiring records to be maintained for 10 years. On March 1, 2023, the DMDC Records and Information Management Branch Chief sent an e-mail DMDC-wide notifying personnel of the policy changes.

(U) The policy changes implemented by the DMDC for retaining financial records supporting SIPRNet token purchases addressed token accountability and traceability problems. Therefore, we did not recommend further corrective actions in this report.

[12] (U) DMDC, "Token Management SOP," Version 2.0, revised November 2022.

(U) Conclusion

(U) We substantiated the DOT&E's concerns and the allegation to the DoD Hotline that the DoD PKI PMO did not have full accountability of SIPRNet tokens. Inaccurate token inventories resulted in the DoD Components purchasing tokens that they may not have needed. As previously discussed, the Army and the Defense Health Agency purchased additional SIPRNet tokens without depleting SIPRNet tokens in the manufacturer's vault that they already purchased. Implementing more stringent controls for managing SIPRNet tokens and maintaining accurate financial records, such as those implemented by the DoD PKI PMO and the DMDC during the audit, improve accountability, enable the DoD to trace tokens to specific purchases, reduce unnecessary expenditures for tokens that may not be needed, and improve financial reporting.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from March 2022 through June 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) To account for SIPRNet tokens, we obtained a universe of SIPRNet token orders from October 2017 through September 2021 to determine whether orders placed through TMS matched the order totals on invoices, MIPRs, and delivery orders. In addition, we verified the number of SIPRNet tokens located in the manufacturer's vault by reviewing the SST Weekly Status Reports and DoD PKI PMO reconciliation reports and comparing it to the results of our reconciliation.

(U) We interviewed personnel from the DoD PKI PMO and the DMDC to understand program management-level processes and controls for ordering and maintaining SIPRNet token inventories. For the DoD Components we reviewed, we interviewed the PKI Program Manager and Leads and RA Officers from the Army, Marine Corps, Navy, Air Force, Defense Information Systems Agency, and DMDC to determine their processes and controls for ordering and accurately accounting for SIPRNet tokens.

(U) We reviewed the following Federal and DoD guidance for maintaining documentation supporting SIPRNet token purchases and inventories of the tokens.

- (U) Federal Acquisition Regulation, Part 4, "Administrative and Information Matters," Subpart 4.805, "Storage, Handling, and Contract Files"
- (U) DoD Regulation 7000.14-R, "DoD Financial Management Regulation"
- (U) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011 (Updated May 18, 2023)

(U) We also nonstatistically selected six DoD Components to verify that SIPRNet tokens were accurately registered in the TMS and that users were in possession of their assigned token. We performed this review at the following DoD Components.

- (U) Headquarters, Department of the Army G-3/5/7, Pentagon, Arlington, Virginia
- (U) U.S. Marine Corps Cyberspace Operations Group, Marine Corps Base Quantico, Quantico, Virginia

- (U) Office of the Chief of Naval Operations for Information Warfare, Pentagon, Arlington, Virginia
- (U) Office of the Chief Information Officer of the Air Force, Pentagon, Arlington, Virginia
- (U) Defense Information Systems Agency Headquarters, Fort George G. Meade, Fort Meade, Maryland
- (U) DMDC, Mark Center, Alexandria, Virginia

(U) We reviewed 107 of 323 users identified by individuals present in their respective offices on the day of testing. We reviewed identification cards, such as Common Access Cards and driver's licenses, to verify the user's identity and compared it to the identity assigned to the SIPRNet token. We also reviewed the user's SIPRNet token identification number to verify that the user held the token registered to them in the TMS.

(U) The DoD Components associated with this oversight project reviewed this report 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 on the CUI treatment of their information. If the DoD Components did not 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) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the DoD PKI PMO and the DMDC processes and controls for managing and accounting for SIPRNet token orders. However, because our review was limited to these internal control components and underlying principles, our review may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We obtained a list of SIPRNet token orders from the TMS from October 2017 through September 2021 to determine whether the DoD accounted for and effectively managed SIPRNet token orders. To assess the reliability of the data, we verified SIPRNet token orders in the TMS to invoices, MIPRs, and delivery orders. However, we did not receive all invoices and MIPRs. Therefore, we could not determine the reliability of all SIPRNet token orders within the TMS during the period of our review.

(U) Prior Coverage

(U) No prior coverage has been conducted on the accountability and management of PKI tokens used to access the SIPRNet during the last 5 years.

(U) Appendix B

(U) SIPRNet Tokens Were Accurately Registered in the TMS, and Users Maintained Control of Assigned Tokens

(U) At the six DoD Components reviewed, DoD Component officials accurately registered SIPRNet tokens to 107 nonstatistically selected users in the TMS, and all users were in possession of their assigned token.

(U) Requirements for SIPRNet Token User Registration and Positive Control of SIPRNet Tokens

~~(CUI)~~ The Office of Management and Budget Memorandum states that Federal agencies must be able to identify, credential, monitor, and manage users that access Federal resources to ensure secure and efficient operations.[13] RA Officers were responsible for issuing SIPRNet tokens after they verify a user's identity and registering the SIPRNet token in the TMS, which includes assigning a user's name and certificate to a SIPRNet token. [redacted] Table 2 lists the number of users, by DoD Component, that we reviewed.

(U) Table 2. Number of Users, by DoD Component, with a SIPRNet Token That We Reviewed

(U) DoD Component	Number of SIPRNet Token Users That We Reviewed
Headquarters, Department of the Army G-3/5/7	11
U.S. Marine Corps Cyberspace Operations Group	13
Office of the Chief of Naval Operations for Information Warfare	32
Office of the Chief Information Officer of the Air Force	10
Defense Information Systems Agency	31
DMDC	10
Total	**107** (U)

(U) Source: The DoD OIG.

[13] (U) Office of Management and Budget M-19-17, "Enabling Mission Delivery through Improved Identity, Credential, and Access Management," May 21, 2019.

[14] (U) The Committee on National Security Systems memorandum, "National Security Systems Public Key Infrastructure Tokens Usage on the Secret Fabric," June 14, 2016.

(U) DoD Components Accurately Registered SIPRNet Tokens, and Users Maintained Positive Control of Them

(U) The Headquarters, Department of the Army G-3/5/7, U.S. Marine Corps Cyberspace Operations Group, Office of the Chief of Naval Operations for Information Warfare, Office of the Chief Information Officer of the Air Force, Defense Information Systems Agency, and the DMDC accurately registered SIPRNet tokens in the TMS for all 107 users reviewed. Specifically, the RA Officer accurately included the required details for each user:

- (U) token certificate's common name, which included user's legal name;
- (U) DoD Component's name;
- (U) certificate status, which could be active, lost, damaged, or compromised; and
- (U) token identification number.

(U) All 107 DoD personnel at the six DoD Components reviewed maintained possession of their assigned SIPRNet token. Maintaining positive control of SIPRNet tokens is essential to the security of classified electronic data up to the SECRET classification level. Compromised or lost SIPRNet tokens with active credentials can be used to obtain unauthorized access to or steal classified information if the personal identification number is also compromised.

(U) Acronyms and Abbreviations

(U) DMDC	Defense Manpower Data Center
(U) DOT&E	Director of Operational Test and Evaluation
(U) MIPR	Military Interdepartmental Purchase Request
(U) PKI	Public Key Infrastructure
(U) PMO	Program Management Office
(U) RA	Registration Authority
(U) SIPRNet	Secret Internet Protocol Router Network
(U) SOP	Standard Operating Procedure
(U) SST	Second Source Token
(U) TMS	Token Management System


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

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